NSH-566

Modularized 24 (100Base-FX) + 2G Access Switch

(Sept. 15, 2006)

Management Guide

COPYRIGHT
All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

FCC WARNING
This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE
This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Take special care to read and understand all content given in the warning boxes

Warning

Table of Contents

1 Introduction 1
Features 1
Specifications 2
2 Web Management Functions 5
2-1. Web Management Home Overview 5
2-2. Denial-of-Service Protection Configuration 6
2-3. Module Type Configuration 6
2-4. Port status 7
2-5. Port Statistics 9
2-6. Administrator 9
2-6-1. IP Address 11
2-6-2. Advanced 11
2-6-3. Console Port Information 13
2-6-4. Port Controls 13
2-6-5. Abnormal Traffic Detection 15
2-6-6. Ethernet Loop Detection 17
2-6-7. Trunking 17
2-6-7-1. Aggregator Setting 18
2-6-7-2. Aggregator Information 19
2-6-7-3. State Activity 20
2-6-8. Filter Database 21
2-6-8-1. IGMP Snooping 21
2-6-8-2. Static MAC Address 22
2-6-8-3. MAC Filtering 23
2-6-9. VLAN Configuration 24
2-6-9-1. Port Based VLAN 26
2-6-9-2. 802.1q VLAN (Tagged Based VLAN) 27
2-6-10. Spanning Tree 33
2-6-11. Port Mirroring 37
2-6-12. SNMP 38
2-6-13. Security Manager 39
2-6-14. TFTP Update Firmware 40
2-6-15. Configuration Backup 41
2-6-15-1. TFTP Backup Configuration 41
2-6-15-2. TFTP Restore Configuration 41
2-6-15-3. TFTP Import Text Configuration File 42
2-6-15-4. TFTP Export Text Configuration File 43
2-6-16. Reboot 43
2-6-17. Network Tree 44
3 Console Xmodem - Update Firmware 45

4 Console Menu Line....48
4-1. Main Menu....48
4-2. Switch Static Configurations....49
4-2-1. Port Configuration....50
4-2-2. Port Abnormal Traffic Detection....51
4-2-3. Ethernet Loop Detection....54
4-2-4. Trunk Configurations....55
4-2-5. VLAN Configuration....57
4-2-5-1. Create a VLAN Group....59
4-2-5-2. Edit / Delete A VLAN Group....61
4-2-5-3. Groups Sort Mode....62
4-2-6. Misc. Configuration....64
4-2-6-1. MAC Age Interval....64
4-2-6-2. Broadcast Storm Filtering....65
4-2-6-3. Max Bridge Transmit Delay Bound....65
4-2-6-4. Port Security....66
4-2-6-5. Collisions Retry Forever....67
4-2-6-6. Hash Algorithm....68
4-2-6-7. Broadcast Filtering....68
4-2-6-8. Module Type Configuration....69
4-2-7. Administration Configuration....70
4-2-7-1. Change Username....70
4-2-7-2. Change Password....71
4-2-7-3. Device Information....71
4-2-7-4. IP Configuration....72
4-2-7-5. Switch Denial-of-Service Protection....72
4-2-7-6. Network Configuration....73
4-2-7-7. Add Static Network Device....73
4-2-8. Port Mirroring Configuration....75
4-2-9. Priority Configuration....76
4-2-9-1. Port Static Priority....76
4-2-9-2. 802.1p Priority Configuration....76
4-2-10. MAC Address Configuration....77
4-2-10-1. Static MAC Address....78
4-2-10-2. Filtering MAC Address....80
4-3. Protocol Related Configuration....83
4-3-1. Spanning Tree Protocol (STP)....84
4-3-1-1.STP Enable....84
4-3-1-2. System Configuration....85
4-3-1-3. Per Port Configurations....85
4-3-2. SNMP....86
4-3-2-1. System Options....87

4-3-2-2. Community Strings 87
4-3-2-3. Trap Managers 88
4-3-3.GVRP 89
4-3-4. IGMP 89
4-3-5. LACP 90
4-3-5-1. Working Port Setting....91
4-3-5-2. State Activity 91
4-3-5-3. LACP Status 92
4-3-6. 802.1x Protocol 93
4-3-6-1. 802.1x Enable....93
4-3-6-2. 802.1x System Configuration....94
4-3-6-3. 802.1x PerPort Configuration 95
4-3-6-4. 802.1x Miscellaneous Configuration 96
4-4. Status and Counters....97
4-4-1. Port Status....97
4-4-2. Port Counters....98
4-4-3. System Information 99
4-4-4. Network Information....100
4-5. Reboot Switch....100
4-5-1. Default....101
4-5-2. Restart....101
4-6. TFTP Update Firmware....101
4-6-1. TFTP Update Firmware....102
4-6-2. Restore Configuration File 102
4-6-3. Backup Configuration File....103
4-6-4. TFTP Import Text Configuration File 104
4-6-5. TFTP Export Text Configuration File....105
5 Menu-Driven Interface via Telnet....107
6 Troubleshooting....108
Appendix A 109
Application Examples 109
Building to Building (Small Campus)....109
Enterprise Server Aggregation....109
Appendix B 111
802.1q Tag-VLAN Application Example 111
Network Topology 112
Appendix C 119
Protocol VLAN Application Example 119
Appendix D 124
System Configuration File Example 124
Contact Us 126

1 Introduction

Emanating from our expertise in developing network communication solutions, the Modularized 24+2G Access Switch incorporates leading-edge switching technology and high port density within a slim 1-rack unit chassis. The Switch represents an industry first as no other switch in the market today can match the unique 3 x 8-Port modules, 2 GBIC slots plus console port design. This innovation offers the ultimate in flexibility and freedom to "mix-and-match" in terms of cabling (fiber + copper) and speed (Ethernet to Gigabit).

Features

- Management via Console, Telnet and Web Browser User Interfaces
- Management via SNMP
- Console and Telnet settings using Menu-Driven Interface
- 3 x 8 10/100 Ethernet plus 2 GBIC uplink ports available
- Support up to 7 trunk groups
- Supports 802.3x flow control for full duplex mode and collision-based backpressure for half-duplex mode
- Supports Head of Line (HOL) blocking prevention
- Supports broadcast storm filtering
- Supports 14k MAC address entries
- Supports port-based VLAN, protocol based VLAN and 802.1q tag-based VLAN
- GVRP
- IGMP Snooping

Specifications

Performance

Throughput: 14,880 pps for 10Mbps Ethernet
148,800 pps for 100Mbps Ethernet
1,488,000 pps for 1000Mbps Ethernet

Max. Distance: UTP: 100 meters (Category 5e or better)

100Mbps Fiber:
2,000 meters (62.5/125 micron fiber cabling)

20,000 meters (9/125 micron fiber cabling)

30,000 meters (9/125 micron fiber cabling)

60,000 meters (9/125 micron fiber cabling)

1000Mbps Fiber:
220 meters (62.5/125 micron fiber cabling)

10,000 meters (9/125 micron fiber cabling)

Connectors and Cabling

Ports: 3x Fast Ethernet slots (for 8-port modules);
2x GBIC

Module Types: 4-port 100Mbps ST, fiber
4-port 100Mbps SC, fiber
8-Port 100Mbps LC, fiber
8-Port 100Mbps MT-RJ, fiber (Produce to order)
8-Port 10/100Mbps RJ-45
8-Port 100Mbps WDM fiber
2-Port Gigabit (GBIC)

Control: Out-of-band control: RS-232
In-band control: RJ-45, Fiber

Power Characteristics

AC Input Voltage: 90 to 240V AC (auto-ranging) 50 to 60 Hz

Output: 3.3V DC, 20A & 5V, 1A (71W)

Environmental Characteristics

Operating:
Temperature: 0°C to 45°C (32°F to 113°F)
Relative Humidity: 5% to 90%, non-condensing

Non-Operating / Storage:

Temperature: -10°C to 70°C (-13°F to 158°F)
Relative Humidity: 5% to 90%, non-condensing

Physical Characteristics

Height: 1.73" (4.4 cm)
Width: 17.32" (44 cm)
Depth: 11.22" (28.5 cm)
Weight: 9.48lbs (4.3kg) fully loaded
Mounting: Standard 19" Rack-mount case

Network Management

System Configuration: Console port, Telnet
Spanning Tree Algorithm: IEEE 802.1d provides redundant link support

Port-based, Protocol-based or 802.1q VLAN's:
Up to 256 VLANs, with GVRP for dynamic VLAN registration

Link Aggregation: up to 4 ports can be combined into a fat pipe, 7 trunks

LEDs:

Modular Ports:

10/100Mbps:	Green, illuminates when data transmission rate 100Mbp
LNK ACT:	Green, flashing or illuminated when link pulses from a compliant device is established, and when transmitting or receiving data packets
FDX:	Amber, illuminated when in full duplex mode

Gigabit Ports:

LNK ACT:	Green, flashing or illuminated when link pulses from a compliant dev ice

Standards and Compliance

IEEE 802.3	10BASE-T specification
IEEE 802.3u	100BASE-TX and 100BASE-FX specification
IEEE 802.3x	Full Duplex on 10BASE-T and 100BASE-TX ports
IEEE 802.3z	1000BASE-SX specification
IEEE 802.1d	Spanning-Tree Protocol
IEEE 802.1p	Priority Queues
IEEE 802.1q	VLAN Tagging
RFC 1350	TFTP

Electromagnetic Compatibility

FCC Part 15 of Class A
CE approved

2 Web Management Functions

The Switch management agent can be access via a web browser, however when setting up the IP or other “first time” settings, it is recommended that you go to section three and use **console** mode to secure a direct connection and to modify them.

Default Address:

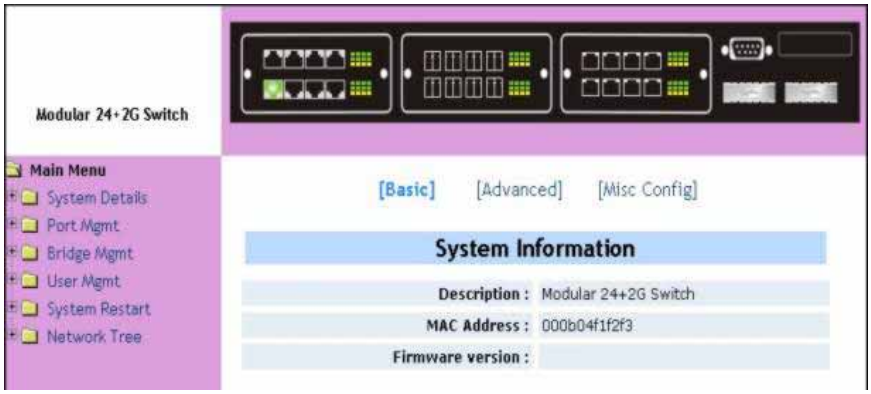
MAC Address:	(Factory set and unique for each device)
IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
User Name:	admin
Password:	(no default password)

The IP address of the Switch used for writing this manual has been set via console mode to 192.168.0.197.

To access the Switch, open a web browser and key in the Switch’s IP address. Enter username and password (default is no password) and click on the <OK> button.

2-1. Web Management Home Overview

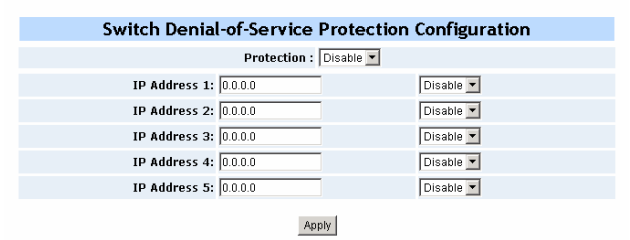
This is the Main Menu Home Page.



Description: Display the name of device type.
MAC Address: The unique hardware address assigned by manufacturer (default)
Firmware Version: Display the Switch's firmware version.

2-2. Denial-of-Service Protection Configuration

The Switch can be protected from denial-of-service attacks. If the user specifies all the IP addresses from which the Switch can be managed, the Switch will discard all management packets from other sources.


Switch Denial-of-Service Protection Configuration
Protection : Disable
IP Address 1: 0.0.0.0 Disable
IP Address 2: 0.0.0.0 Disable
IP Address 3: 0.0.0.0 Disable
IP Address 4: 0.0.0.0 Disable
IP Address 5: 0.0.0.0 Disable
Apply

This function can be enabled or disabled. The selected IP addresses will be granted management rights.

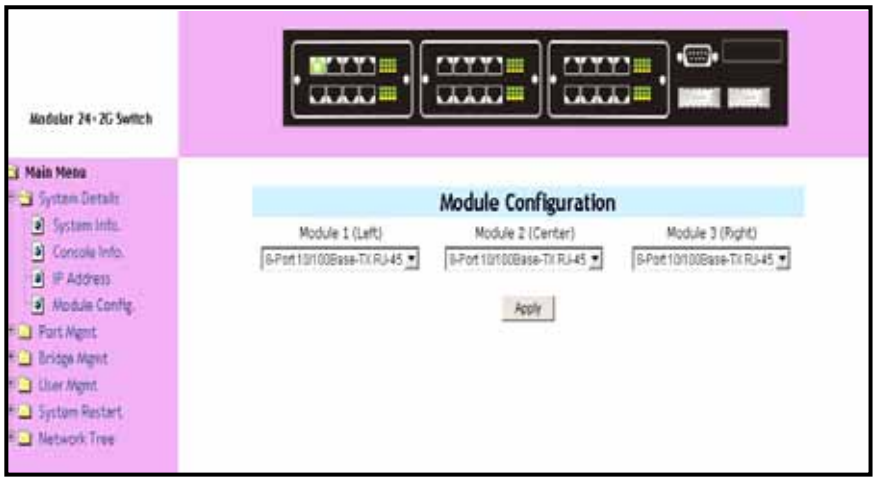
2-3. Module Type Configuration

The switch is modularized. In addition to two GBIC ports, there are three modules selectable for your needs. For the different type modules, some module/port settings maybe need to be reconfigured. You can configure the module type by this function. The system can also configure all the

port settings of the module to the pre-defined values for you. If some of the detail settings of each port do not meet your needs, you can change them on a port-by-port basis from the **Port Controls Page**. The default module type is 8-port 10/100 Base-TX RJ-45.

Available module types:

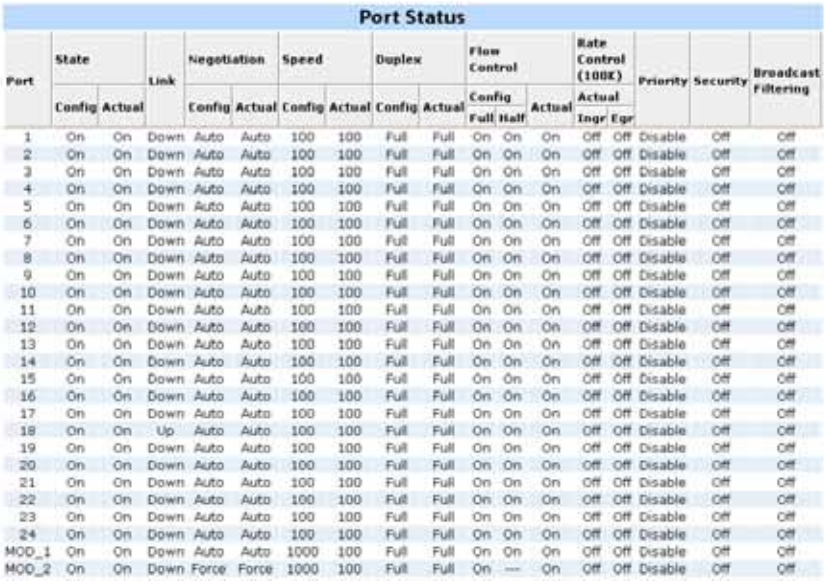
1. No Module
2. 8-Port 10/100 Base-TX RJ-45
3. 4-Port 100 Base-FX ST/SC
4. 8-Port 100 Base-FX LC
5. 8-Port 100 Base-FX MT-RJ
6. 8-Port 100 Base-FX BiDi



Warning: The modules are not hot-swappable. You must turn off the power before you change the modules. Failure to do so may result in damage to the Switch.

2-4. Port status

This screen shows every port status that was set by the user – and the negotiation results.



Port Status

Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control (100K)		Priority	Security	Broadcast Filtering
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config		Actual	Actual				
										Full	Half		Ingr	Egr			
1	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
2	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
5	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
6	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
7	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
8	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
9	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
10	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
11	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
12	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
13	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
14	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
15	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
16	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
17	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
18	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
19	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
20	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
21	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
22	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
23	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
24	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
MOD_1	On	On	Down	Auto	Auto	1000	100	Full	Full	On	On	On	Off	Off	Disable	Off	Off
MOD_2	On	On	Down	Force	Force	1000	100	Full	Full	On	---	On	Off	Off	Disable	Off	Off

1. **State:** Displays port statuses disable or enable. “unlink” will be treated as “off ”.

2. **Link Status:** Down is “No Link”, UP is “Link”.

3. **Auto-Negotiation:** Display the auto-negotiation mode: auto/force/NWay.

4. **Speed status:** Display 1000Mbps or 100Mbps or 10Mbps speed, port 1- 24 are 10/100Mbps (depending on the modular card used), port 25-26 are 1000Mbps.

5. **Duplex status:** Display full duplex or half-duplex mode.

6. **Flow Control:**
   Full: Display the flow control status is enabled or disabled in full mode.
   Half: Display the backpressure is enabled or disabled in half mode.

7. **Rate Control:** Display the rate control setting.
   Ingr: Display the port effective ingress rate of user setting.
   Egr: Display the port effective egress rate of user setting.

8. **Priority:** Display the port static priority status is High or Low or disable.

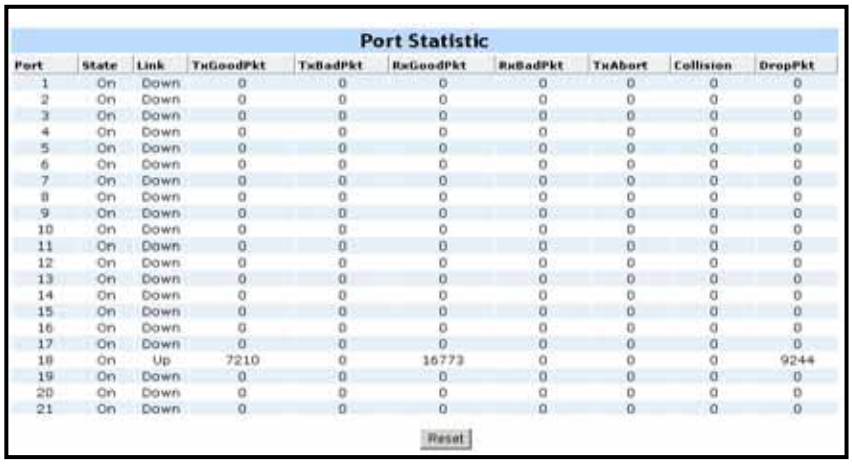
9. **Port Security:** Display the port security is enabled or disabled.

10. **Config:** Display the state of user setting.

11. **Actual:** Display the negotiated result.

2-5. Port Statistics

Port statistics provide a summary of the current switch's status, including on/off state, link status, good or bad packets transmitting and receiving, aborted packets, collisions and dropped packets.



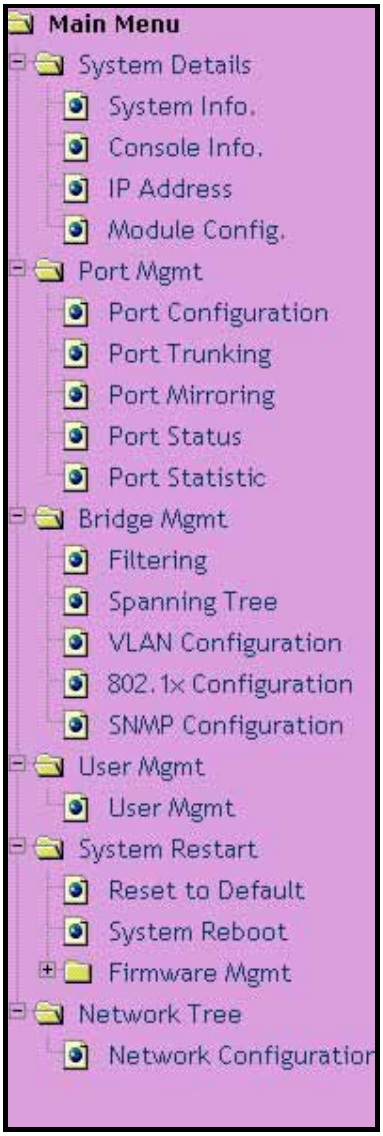
Port Statistic

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1	On	Down	0	0	0	0	0	0	0
2	On	Down	0	0	0	0	0	0	0
3	On	Down	0	0	0	0	0	0	0
4	On	Down	0	0	0	0	0	0	0
5	On	Down	0	0	0	0	0	0	0
6	On	Down	0	0	0	0	0	0	0
7	On	Down	0	0	0	0	0	0	0
8	On	Down	0	0	0	0	0	0	0
9	On	Down	0	0	0	0	0	0	0
10	On	Down	0	0	0	0	0	0	0
11	On	Down	0	0	0	0	0	0	0
12	On	Down	0	0	0	0	0	0	0
13	On	Down	0	0	0	0	0	0	0
14	On	Down	0	0	0	0	0	0	0
15	On	Down	0	0	0	0	0	0	0
16	On	Down	0	0	0	0	0	0	0
17	On	Down	0	0	0	0	0	0	0
18	On	Up	7210	0	16773	0	0	0	9244
19	On	Down	0	0	0	0	0	0	0
20	On	Down	0	0	0	0	0	0	0
21	On	Down	0	0	0	0	0	0	0

Reset

2-6. Administrator

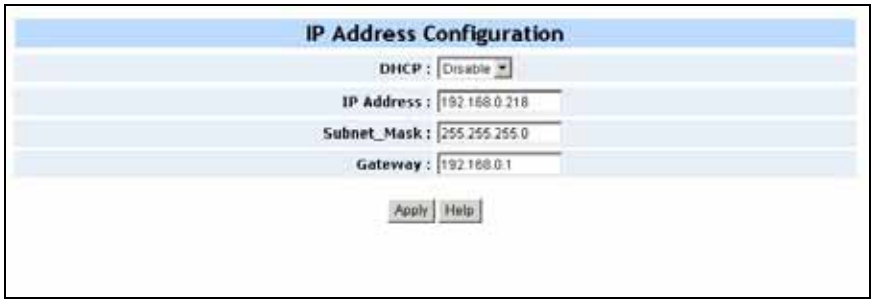
There are many management functions that could be accessed via the web browser. The main menu system lists all the functions. Simply click on each item to go to the appropriate page.



2-6-1. IP Address

The user can manually configure the IP Settings. Simply click on the IP address field and enter the address, then click the “Apply” button to change the address.

Note: The user must reset/restart the Switch in order to use the new IP address setting.



2-6-2. Advanced

Miscellaneous Setting:

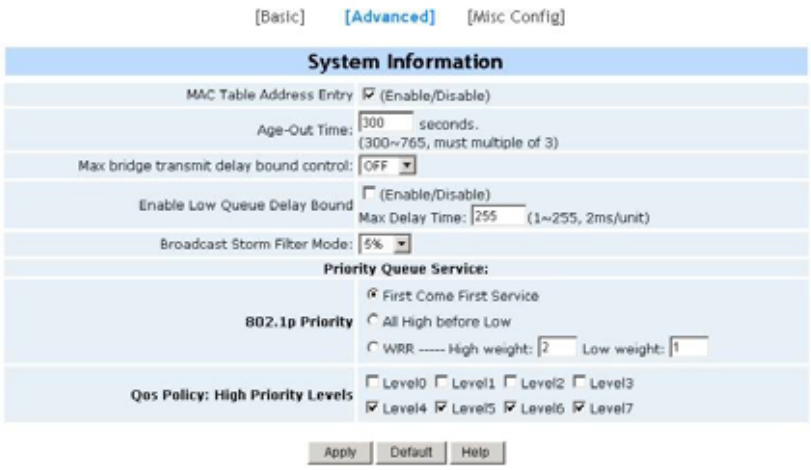
MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the Switch's address table. The valid range is 300~765 seconds. The default is 300 seconds.

Max bridge transmit delay bound control: Limit the packets queuing time in the Switch. If enable, the packets queued exceed this time will be dropped. The valid values are 1 sec, 2 sec, 4 sec and off.

Enable Low Queue Delay Bound: Limit the low priority packets queuing time in the Switch. If the low priority packets stay in the Switch exceed the Max Delay Time, it will be sent. The valid range is 1~255 ms.

NOTE: Make sure that “Max bridge transit delay bound control” is enabled before activating the Delay Bound.

Broadcast Storm Filter: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above this threshold, broadcast storm control will activate. The valid threshold values are 5%, 10%, 15%, 20%, 25% and OFF.



Priority Queue Service settings:

First Come First Service (FCFS): The sequence of packets sent depends on the order they arrive.

All High before Low (AHBL): The high priority packets are sent before low priority packets.

Weighted Round Robin (WRR): Select the preferred ratio of high and low priority packets sent by the Switch in its priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, 5 High: 2 Low, means that the Switch sends 5 high priority packets before sending 2 low priority packet.

QoS Policy - Priority Levels: 0~7 QoS levels can be assigned to designated high or low priority.

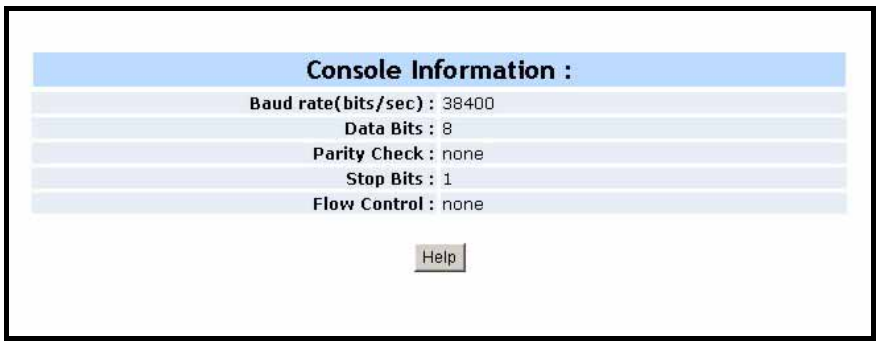
Collisions Retry Forever: Disable – In half-duplex, if collision occurs,

the Switch will retry send 48 times before dropping the frame.
Enable – In half-duplex, if collision occurs, the Switch will retry to send packets indefinitely.

2-6-3. Console Port Information

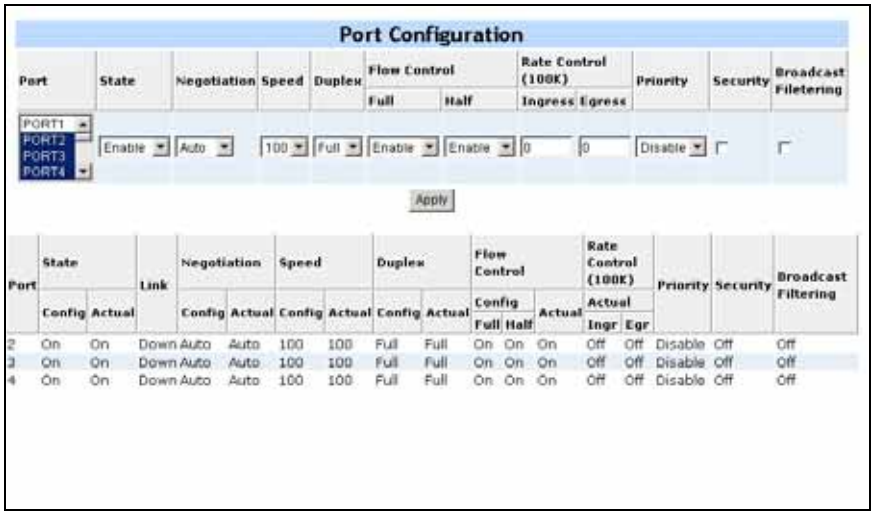
Console is a standard UART interface to communicate with the Serial Port. The user can launch windows HyperTerminal program to link with the Switch. See section three for details

Bits per seconds: 38400
Data bits: 8
Parity: none
Stop Bits: 1
Flow control: none



2-6-4. Port Controls

Use this page to change the status of each port.



Explanation of Fields:

1. **State:** User can disable or enable this port control.

2. **Auto-Negotiation:** User can set auto-negotiation modes:

   a. Force - specify the speed/duplex on this port
   b. NWay Force - specify the speed/duplex on this port with auto-negotiation enabled.
   c. Auto – for the Switch to automatically determine the highest speed and duplex mode possible

3. **Speed:** User can set 100Mbps or 10Mbps speed on Port1~Port24 (depending on module card specifications), 1000Mbps speed on port25~port26.

4. **Duplex:** User can set full duplex or half-duplex mode for each port.

5. **Flows control:**
   Full: User can set full - flow control function (pause).
   Half: User can set half – flow control (backpressure).

6. **Rate Control:** port1 ~ port 24, supports by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate to 1Mbps, ingress rate is 500Kbps. The Switch

will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

Ingress: Type the port effective ingress rate. The valid range is 0 ~ 1000. The unit is 100Kbps
0: disable rate control. (i.e. no rate limitation)
1 ~ 1000: valid rate value

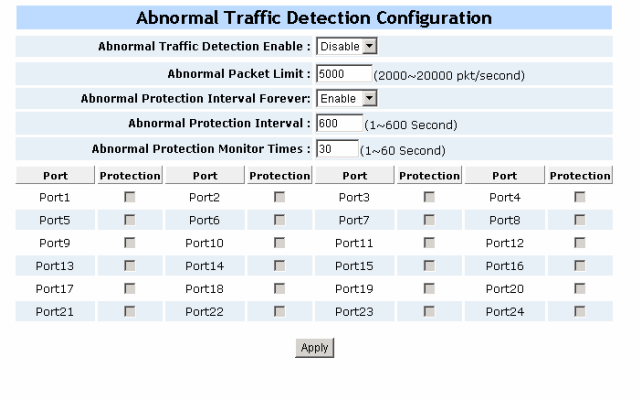
Egress: Type the port effective egress rate. The valid range is 0~1000. The unit is 100Kbps.
0: disable rate control.
1 ~ 1000: valid rate value.

7. **Priority:** This static priority based on port, if you set the port to high priority, the priority of incoming packets to this port will always be high.

8. **Port Security:** A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded. User can disable the port from learning any new MAC addresses, and then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, and then click "Apply" to set the Switch.

2-6-5. Abnormal Traffic Detection

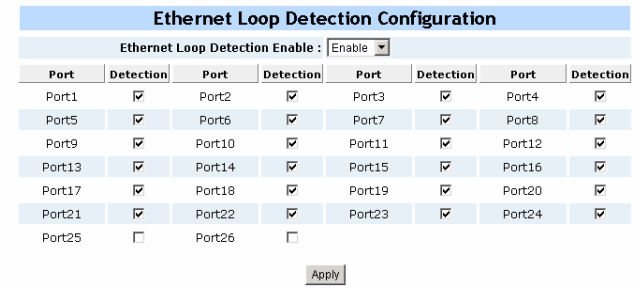
The Abnormal Traffic Detection function allows the user to configure the bandwidth threshold up to which the specified ports can receive broadcast packets. If the incoming broadcast packets exceed this limit, the Switch can disable that port for a specified time or permanently ('forever').


Abnormal Traffic Detection Configuration
Abnormal Traffic Detection Enable : Disable
Abnormal Packet Limit : 5000 (2000~20000 pkt/second)
Abnormal Protection Interval Forever: Enable
Abnormal Protection Interval : 600 (1~600 Second)
Abnormal Protection Monitor Times : 30 (1~60 Second)
Port Protection Port Protection Port Protection Port Protection
Port1 Port2 Port3 Port4
Port5 Port6 Port7 Port8
Port9 Port10 Port11 Port12
Port13 Port14 Port15 Port16
Port17 Port18 Port19 Port20
Port21 Port22 Port23 Port24
Apply

Attribute	Meaning
Abnormal Traffic Detection Enable	“Enable” or “Disable” this function
Abnormal Packet Limit	The bandwidth threshold for incoming broadcast packets
Abnormal Protection Interval Forever	Enable: Disable the port forever if the incoming broadcast packets exceed the bandwidth threshold continuously in the specified monitor time interval. Disable: Disable the port only for a specified time interval if the incoming broadcast packets exceed the bandwidth threshold continuously in the specified monitor time interval
Abnormal Protection Interval	The time period that the port will be disabled if the incoming broadcast packets exceed the bandwidth limit
Abnormal Protection Monitor Times	The period over which a port must experience an overflow of broadcast packets before being disabled
Port / Protection	Enable or Disable the Abnormal Traffic Detection function per port

2-6-6. Ethernet Loop Detection

The Ethernet Loop Detection function provides a means to detect the loop condition on the sub-network connected to the port. If such a condition is detected, the port will be disabled by the Switch.


Ethernet Loop Detection Configuration
Ethernet Loop Detection Enable : Enable
Port Detection Port Detection Port Detection Port Detection
Port1 Port2 Port3 Port4
Port5 Port6 Port7 Port8
Port9 Port10 Port11 Port12
Port13 Port14 Port15 Port16
Port17 Port18 Port19 Port20
Port21 Port22 Port23 Port24
Port25 Port26
Apply

Users can enable or disable the function for the whole Switch or per port. If the port is disabled because the loop condition has been detected, the port needs to be enabled again manually.

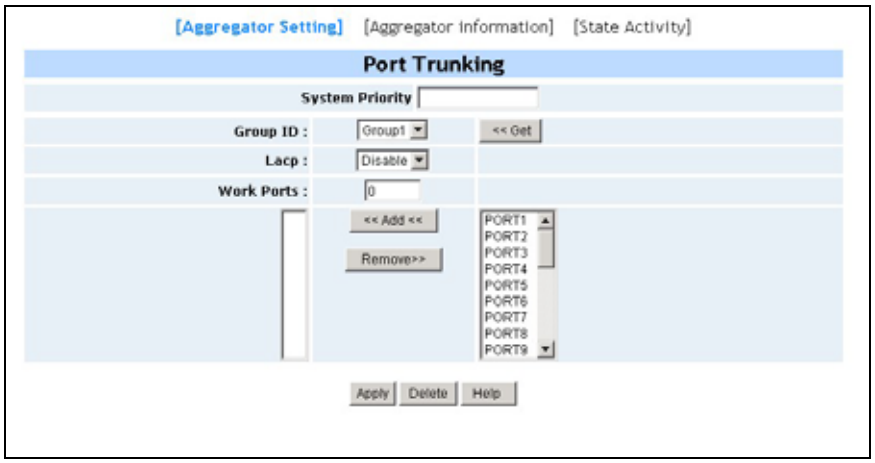
2-6-7. Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs. Move the link to that Aggregation Group and enable its transmission and reception functions in an orderly manner.

Link Aggregation lets you group up to four ports into a single dedicated connection. If more than four ports attached to the same Switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails. All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation. This feature can expand bandwidth to a device on the network. **LACP operation requires full duplex mode,** for more detailed

information, please refer to IEEE 802.3ad.

2-6-7-1. Aggregator Setting



1. **System Priority:** LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

   a. Ports must be configured with the same system priority to join the same LAG.
   b. System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
   c. Given a pair of Switches trunked together, the switch with the lowest system priority value has the highest priority and will behave as the active LACP.

2. **Group ID:** There are seven trunk groups to provide configures. Choose the "group id" and click "Get".
3. **LACP:** If enable, the group is LACP static trunking group. If disabled, the group is local static trunking group. All ports support LACP dynamic trunking groups. If connecting to a device that also supports LACP, the LACP dynamic trunking group will be created automatically.
4. **Work ports:** Work ports are typically a subset of the total ports

selected for trunking. They are the primary working ports during normal operation. The switch allows for a maximum of four ports which can be aggregated at the same time. If LACP static trunking group is active, the surplus ports function as standby and are able to aggregate if any work ports fail. If local static trunking group is active, the number of work ports must be the same as the group member ports.

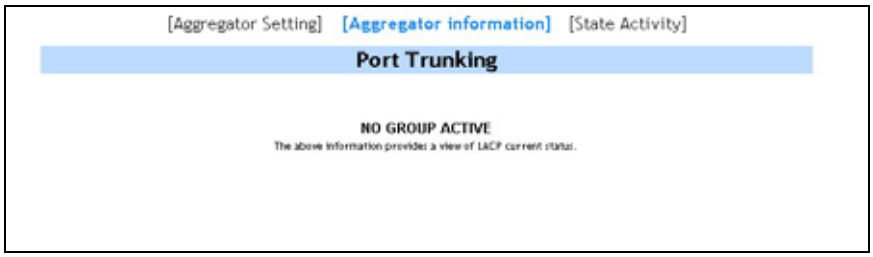
To form a trunking group, simply select the ports to join the trunking group from the available ports list on the right pane. Click <<Add<< to add the port to the group. A maximum of four ports can be aggregated to any group. If LACP is enabled, you can configure LACP Active/Passive status in each port on State Activity page.

5. Click "Apply."

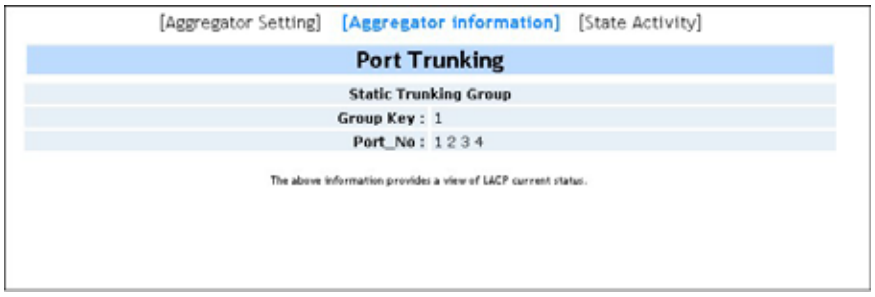
2-6-7-2. Aggregator Information

When setting LACP aggregator, you can view related information from "Aggregator Information" as follows.

1. This page provides LACP current status. In this case, NO GROUP ACTIVE, since LACP is not enabled.



2. This page displays Static Trunking groups.

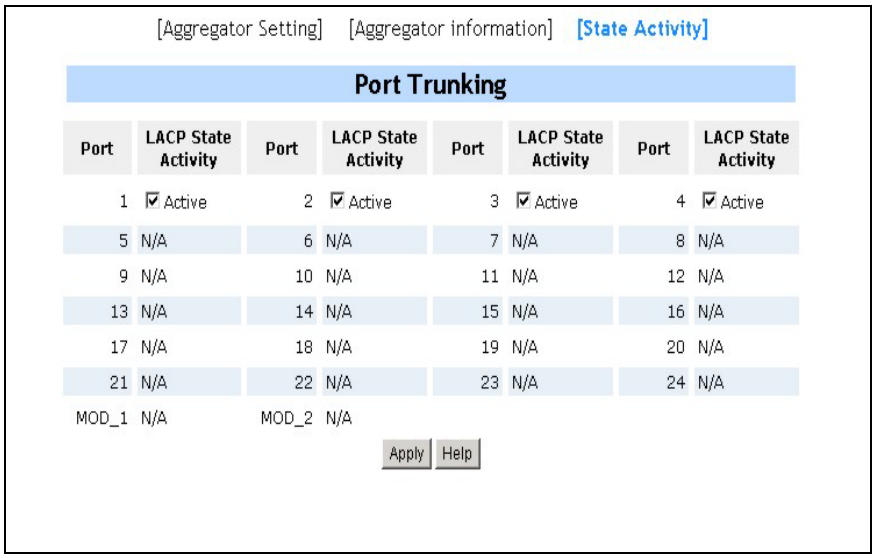

[Aggregator Setting] [Aggregator information] [State Activity]
Port Trunking
Static Trunking Group
Group Key : 1
Port_No : 1 2 3 4
The above information provides a view of LACP current status.

2-6-7-3. State Activity

Active (select)**:** The port automatically sends LACP packets.
Passive (no select)**:** The port does not automatically send LACP packets, and respond only if it receives LACP packets from another networking device.

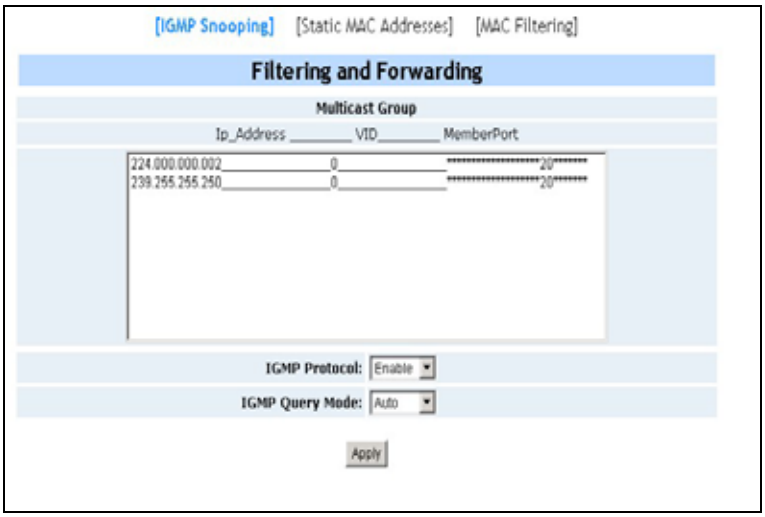
A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for LACP packet from another networking device.

If the switch is set to be an active LACP's actor, **and** ports are selected for trunking (from the Port Trunking > Aggregator Settings, shown in the previous section) then all ports selected to participate in trunking that port's LACP State will be automatically set to Active in the screen below. The LACP State Activity may be inactivated by un-checking the status box next to the port.


[Aggregator Setting] [Aggregator information] [State Activity]
Port Trunking
Port LACP State Activity Port LACP State Activity Port LACP State Activity Port LACP State Activity
1 Active 2 Active 3 Active 4 Active
5 N/A 6 N/A 7 N/A 8 N/A
9 N/A 10 N/A 11 N/A 12 N/A
13 N/A 14 N/A 15 N/A 16 N/A
17 N/A 18 N/A 19 N/A 20 N/A
21 N/A 22 N/A 23 N/A 24 N/A
MOD_1 N/A MOD_2 N/A
Apply Help

2-6-8. Filter Database

2-6-8-1. IGMP Snooping

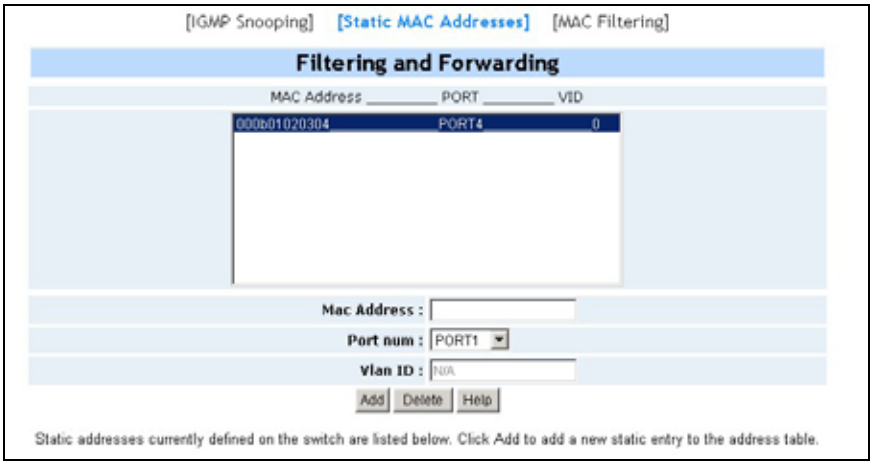


The Switch supports IP multicast, you can enable IGMP on the Filtering and Forwarding > IGMP Snooping page (shown above). You can view different multicast group, VID and member ports here. IP multicast addresses range from 224.0.0.0 to 239.255.255.255.
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the Switch. IGMP have three fundamental types of messages. See table below:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

2-6-8-2. Static MAC Address

When you add a static MAC address, it is stored in the Switch's address table regardless of whether the device is physically connected to the Switch. This saves the Switch from having to re-learn a device's MAC address when the device is disconnected or powered-off, and is then active in the network again.

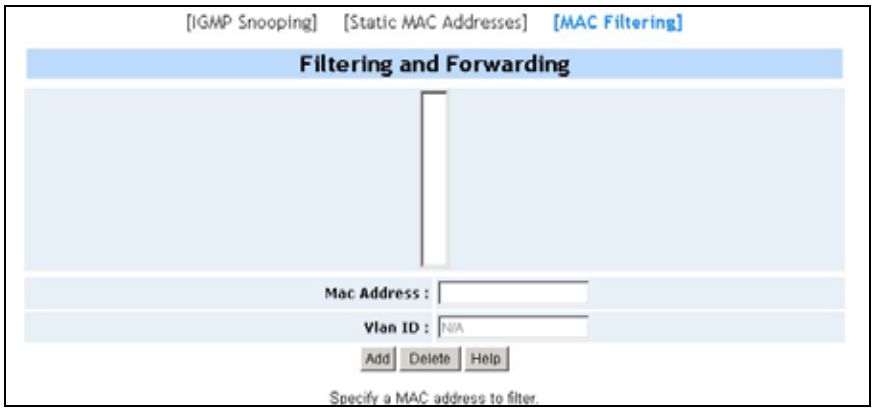


Adding a new static MAC address

1. From the main menu, click Administrator Filter Database Static MAC Address.
2. In the MAC address box, enter the MAC address to and from which the port should permanently forward traffic, regardless of the device's network activity.
3. In the Port Number box, enter a port number.
4. If tag-based (IEEE 802.1q) VLANs are set up on the Switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) associated with the MAC address.
5. Click on the "Add" button.

2-6-8-3. MAC Filtering

MAC address filtering allows the Switch to drop unwanted traffic. Traffic is filtered based on the destination addresses.

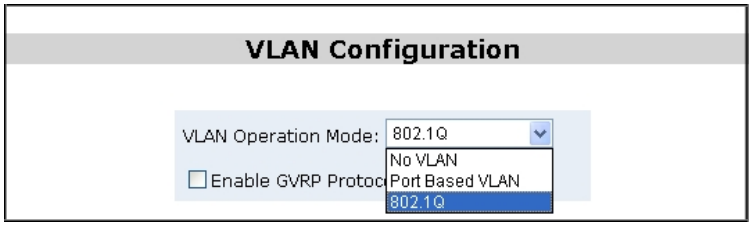


Filtering a MAC address

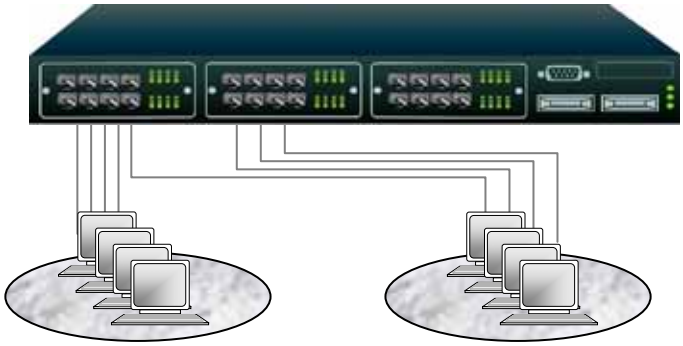
1. In the MAC Address box, enter the MAC addresses that are to be filtered.
2. If tag-based (802.1q) VLAN are set up on the Switch, in the VLAN ID box type the VID associated with the MAC address.
3. Click the on "Add" button.
4. Choose the MAC address that you want to delete and then click on the "Delete" button.

2-6-9. VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN in a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically. The Switch supports port-based, 802.1q (tagged-based) and protocol-based VLAN in web management page. In the default configuration, VLAN support is disabled. There are a few configuration examples in Appendix B for your reference.



Support Port-based VLAN
Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.



GROUP 1
SALES

GROUP 2
R&D

Support Tag-based VLAN (IEEE 802.1q VLAN)

Tagged-based VLAN is an IEEE 802.1q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tags contain a VLAN Identifier (VID) that represents the VLAN numerically.

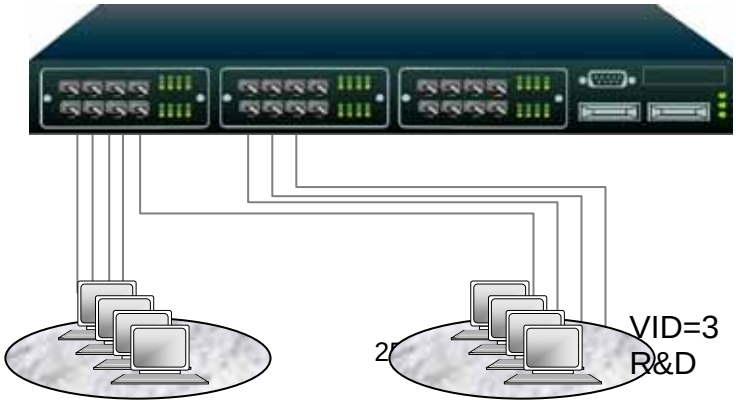
Support Protocol-based VLAN

In order for an end station to send packets to different VLANs, it has to either:

a. Be capable of tagging packets it sends with VLAN tags, OR
b. Be attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, including its protocol (such as Novell IPX and AppleTalk’s EtherTalk)

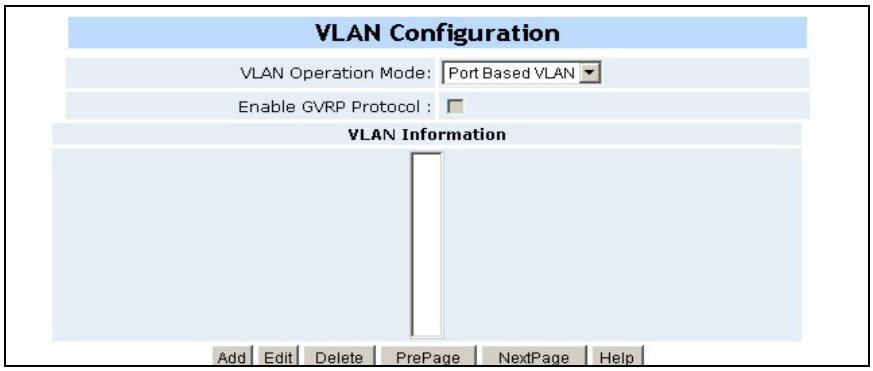
The feature can be applied for accommodating devices that you want to participate in the VLAN, but don’t support tagging. Therefore, the system can add VLAN tags to untagged frames which are based on PVID or on different protocols. (Please see next section for PVID introduction and configuration)

The Switch will support protocol-based VLAN classification by means of both built-in knowledge of layer 2 packet formats used by selected popular protocols, such as Novell IPX and AppleTalk’s EtherTalk, and some degree of programmable protocol matching capability. A port can join more than one different protocol VLANs, but a port can’t apply a same protocol twice for the VLAN configuration purpose. Otherwise you will see the error message: “Save fail for ethertype conflict” when trying to configure VLANs.



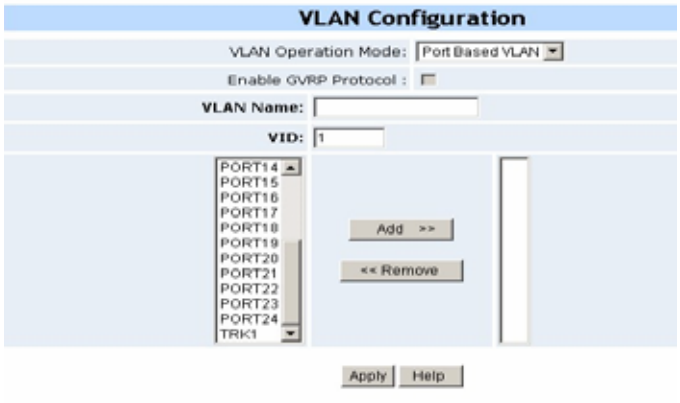
VID=2
SALES

2-6-9-1. Port Based VLAN



Create a new port-based VLAN

1. Click Add to create a new VLAN group.
2. Enter the VLAN name, group ID and select the members for the new VLAN.
3. Click Apply.
4. If there are many groups that over the limit of one page, you can click the “NextPage” to view other VLAN groups.



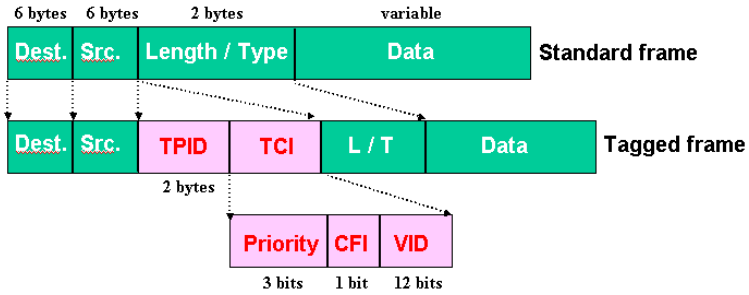
Adding Ports and Trunks to the VLAN

For Port Based VLANs, all available ports (or trunks) which may participate in a VLAN can be selected for participation in the Port Based VLAN Configuration screen shown above. If trunk groups exist, they are displayed as: TRK1, TRK2, etc. and displayed along with the Switches ports in the left hand side panel. You can combine trunk groups and ports together to form a VLAN simply by selecting the available ports trunks from the left panel, and pressing the Add>> button. Remove ports or trunks by selecting and pressing <<Remove. When finished, press Apply.

2-6-9-2. 802.1q VLAN (Tagged Based VLAN)

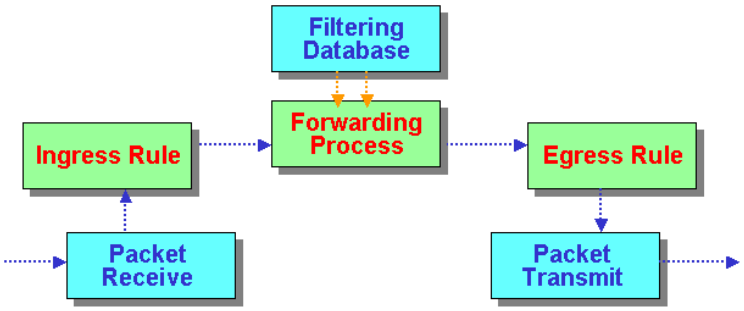
Before going into setting tag-based VLAN, let's first briefly discuss the concepts. For readers who are familiar with the details of tag-based VLAN, you may skip this section and go right to "How to set tag-based VLAN".

For IEEE 802.1q standard, Tag-based VLAN uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame. It contains two bytes of TPID (Tag Protocol Identifier) and two bytes of TCI (Tag Control Information). These four bytes reside within the type/length field of the Ethernet frame that starts after the source address field of the Ethernet frame.



How 802.1q VLAN works

According to the VID information in the tag, the switch forward and filter the frames among ports. These ports with same VID can communicate with each other. IEEE 802.1q VLAN functions contains the following three tasks, Ingress Process, Forwarding Process and Egress Process.



1. Ingress Process:

Each port is capable of passing tagged or untagged frames. Ingress Process identifies if the incoming frames contain tag, and classifies the incoming frames belonging to a VLAN. Each port has its own Ingress rule. If Ingress rule accept tagged frames only, the switch port will drop all incoming non-tagged frames.

a. When a tagged frame is received on a port, it carries a tag header that has a explicit VID. Ingress Process directly passes the tagged frame to Forwarding Process.
b. An untagged frame doesn't carry any VID to which it belongs. When a untagged frame is received, Ingress Process insert a tag contained the PVID into the untagged frame. Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

After Ingress Process, all frames have 4-bytes tag and VID information, and then go to Forwarding Process.

2. Forwarding Process:

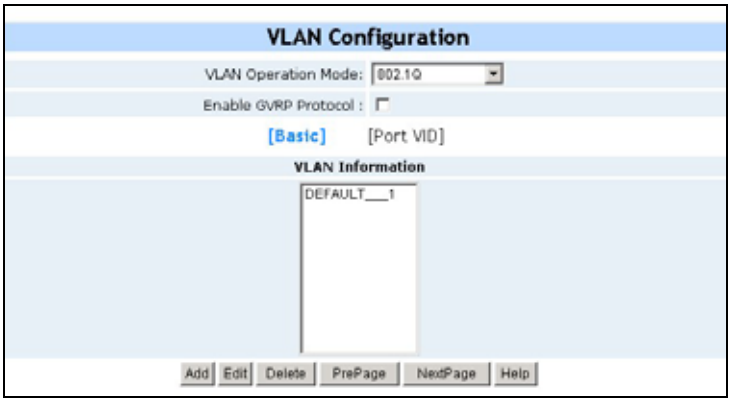
The Forwarding Process decides to forward the received frames according to the Filtering Database. If you want to allow the tagged frames can be forwarded to certain port, this port must be the egress port of this VID. The egress port is an outgoing port for the specified VLAN, that is, frames with specified VID tag can go through this port. The Filtering Database stores and organizes VLAN registration information useful for switching frames to and from switch ports in the DVLAN table. The DVLAN table is automatically learned via GVRP protocol, and can't be created and upgraded by the administrator.

3. Egress Process:

The Egress Process decides if the outgoing frames but be sent tagged or untagged. Egress Process refers to the egress tag control information in Filtering Database. If the value is tagged, the outgoing frame on the egress port is tagged. If the value is untagged, the tag will be removed before frame leaves the egress port.

How to create tag-based VLANS and enable/disable GVRP protocol

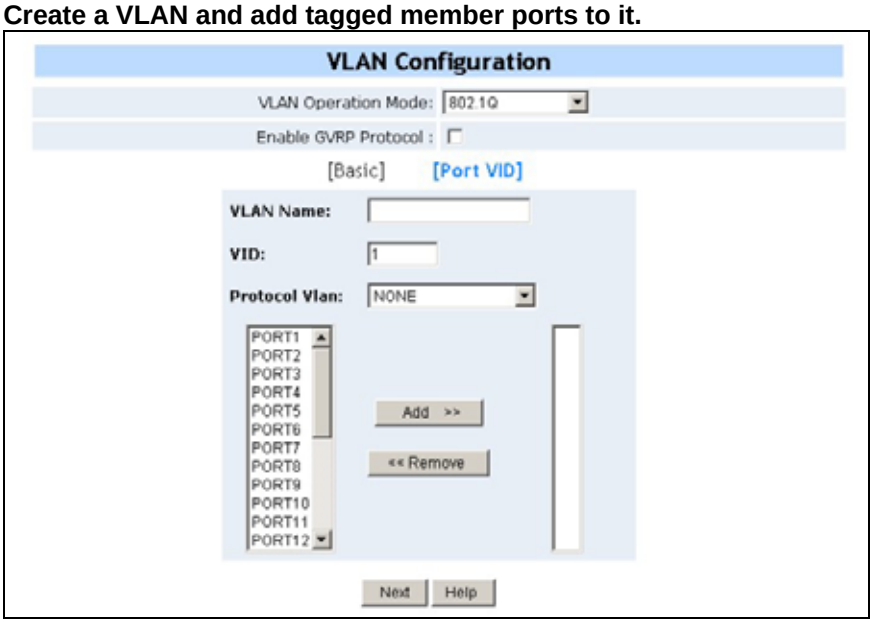
Open the VLAN Configuration Screen and select 802.1q from the “VLAN Operation Mode”. There are 256 VLAN groups available in the Switch. Enable 802.1q VLAN, all ports on the Switch belong to a default VLAN. Its VID is 1. The default VLAN cannot be deleted.



GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)

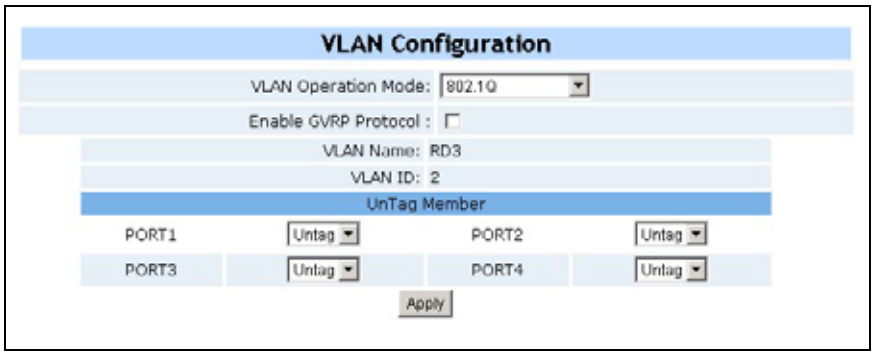
GVRP allows automatic VLAN configuration between the Switch and nodes. If the Switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the Switch. The Switch will automatically add that device to the existing VLAN.

Create a VLAN and add tagged member ports to it.



The above screen is the Main Tag-based VLAN (802.1q) page

1. From the main menu, click Administrator VLAN configuration, click Add then you will see the page as above.
2. Type a name for the new VLAN.
3. Type a VID number (between 2-4094). The default is 1 (In total, there are 255 VLANs that can be configured).
4. Choose the protocol type. If you are not applying protocol VLAN, you must set the value to “NONE”. You can’t set a port to join more than one VLANs/VIDs with a same protocol.
5. From the Available ports box, select ports to add to the Switch and click “Add >>”. If the trunk groups exist, you can see displayed as: TRK1, TRK2, …, …, and you can configure it to be a member of the VLAN or not.
6. Click “Next.” Then you can view the page as follows.



7. After adding ports to the VLAN, you use the above page to set the outgoing frames as VLAN-tagged frames or not. The default is ‘Untag’. Using the dropdown box, select ‘Tag’ or ‘Untag’ and click “Apply.”

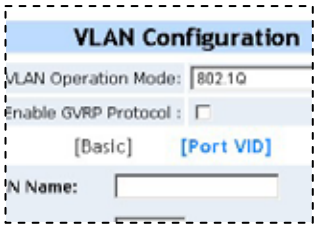
Note: Unless you are sure the network has no tag-unaware devices, you should leave the default setting of the outgoing frames to “Untag”.

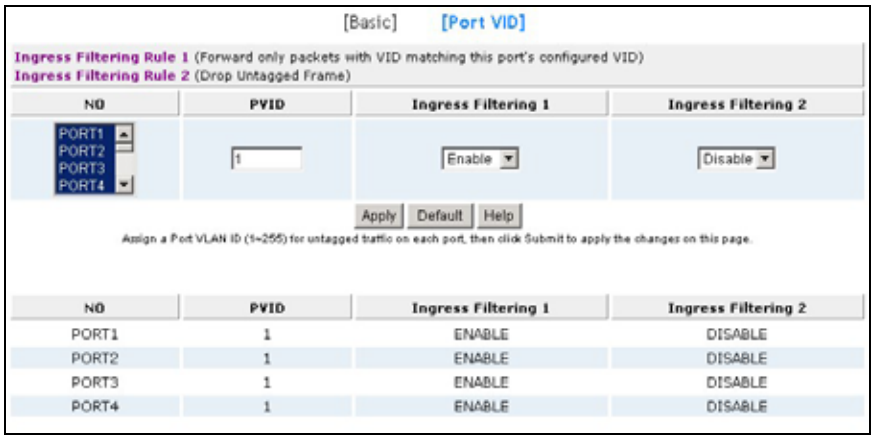
Tag: Outgoing frames with VLAN-tagging.
Untag: Outgoing frames without VLAN-tagging.

Configure port VID settings

From the main tag-based (IEEE 802.1q) VLAN page, click Port VID Settings. Configure port VID settings

From the Main Tag-based VLAN page, click [Port VID] (shown on the insert to the right) to enter the Port VID Settings menu.




[Basic] [Port VID]
Ingress Filtering Rule 1 (Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2 (Drop Untagged Frame)
NO PVID Ingress Filtering 1 Ingress Filtering 2
PORT1 PORT2 PORT3 PORT4
1
Enable
Disable
Apply Default Help
Assign a Port VLAN ID (1~255) for untagged traffic on each port, then click Submit to apply the changes on this page.
NO PVID Ingress Filtering 1 Ingress Filtering 2
PORT1 1 ENABLE DISABLE
PORT2 1 ENABLE DISABLE
PORT3 1 ENABLE DISABLE
PORT4 1 ENABLE DISABLE

Port VID (PVID)

Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Each port allows user to set one PVID, the range is 1~4095, default PVID is 1.

Ports may share a same PVID, but all the PVIDs of the ports on the switch must belong to the **same 256 number group segment.** (For example: 1~255, 256~511,…3840~4095). This is in order to allow for faster Ingress processing of frames. The PVID will be used for VLAN ID tagging to untagged frames.

Note also that the PVID must be the same as the member VLAN group IDs that the port belongs to, else the untagged traffic will be dropped. This is because the port can't transmit a frame with a VLAN Group ID it

doesn't belong to. If a port also joins a protocol VLAN, the Switch will apply the protocol VLAN ID to untagged frames first. If the frame doesn't meet one of the protocols the port has defined, then the PVID will be applied for this frame.

Ingress Filtering
Ingress filtering lets frames belonging to a specific VLAN to be forwarded. The Switch has two ingress filtering rules as follows:

Rule 1: Forward only packets with VID matching this port's configured VID. The default is "Enable". By default, only the packets with VID matching this port's configured VID can pass the port.
Rule 2: Drop Untagged Packet. The default is "Disable". By default, untagged packets can pass the port.

2-6-10. Spanning Tree

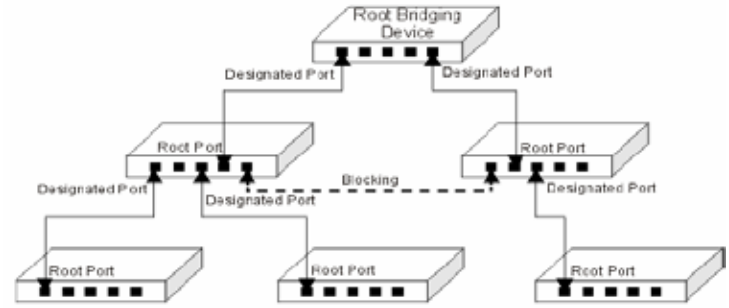
The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switched networks. When STP is enabled, it ensures that only one path at a time is active between any two nodes in the network. You can enable Spanning Tree Protocol by checking the "STP State" check box from the Spanning Tree Configuration > System Configuration menu (shown below). We recommend that you enable STP on all switches to ensure that only a single active path in the network exists.

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designate bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval

(Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.



1. From the Spanning Tree Configuration Menu (shown below), you can create a new value for the STP parameter, and then click the "Apply" button to set it. You can view spanning tree information the Root Bridge device from the same screen.

[System Configuration] [PerPort Configuration]

Spanning Tree Configuration

Configure Spanning Tree Parameters

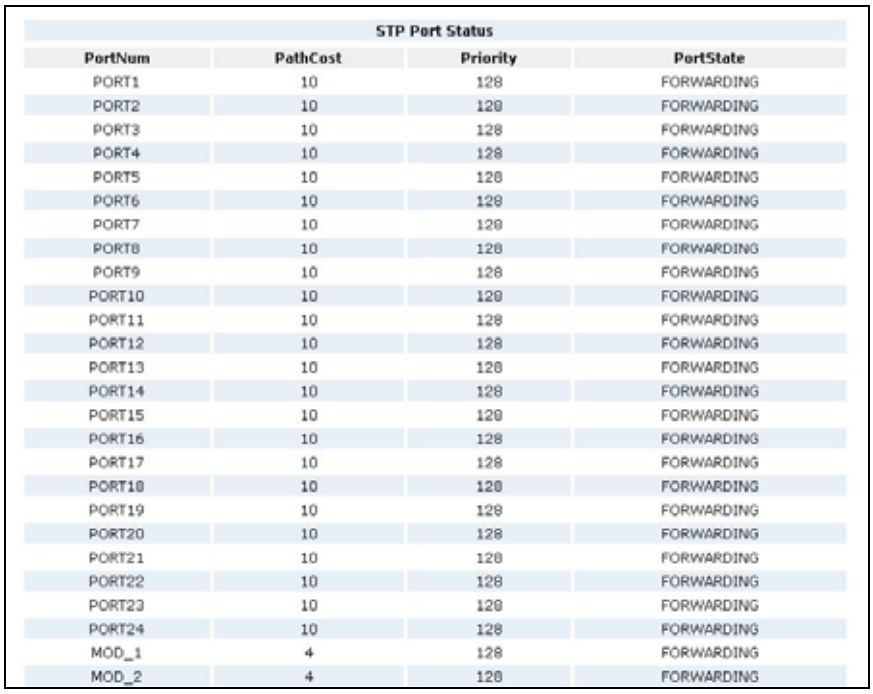
STP State	☑
Priority (0-65535)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward_Delay_Time(4-30)	15

Apply

Spanning Tree Configuration

Priority	32760
Mac Address	0050bf124ba0
Root_Path_Cost	10
Root Port	PORT10
Max Age	10
Hello Time	2
Forward Delay	7

You can view spanning tree status about the Switch from the following screen.



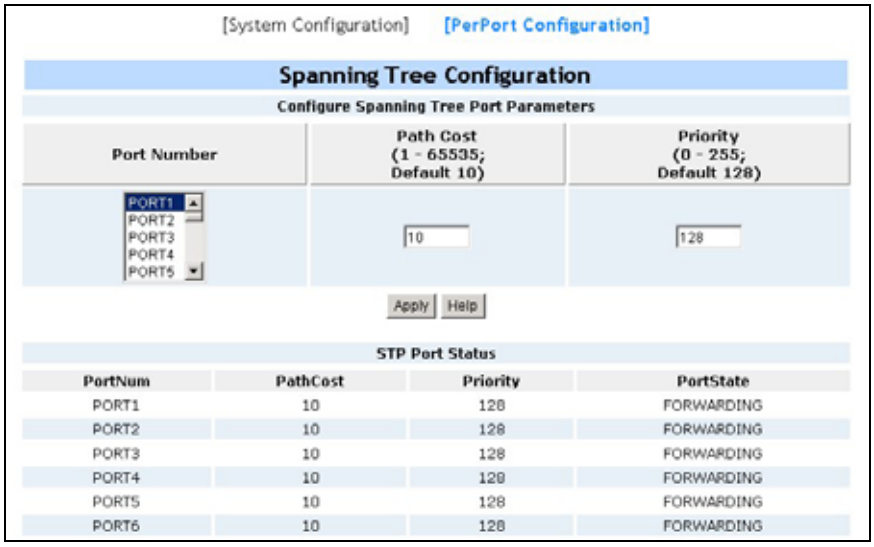
STP Port Status

PortNum	PathCost	Priority	PortState
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING
PORT6	10	128	FORWARDING
PORT7	10	128	FORWARDING
PORT8	10	128	FORWARDING
PORT9	10	128	FORWARDING
PORT10	10	128	FORWARDING
PORT11	10	128	FORWARDING
PORT12	10	128	FORWARDING
PORT13	10	128	FORWARDING
PORT14	10	128	FORWARDING
PORT15	10	128	FORWARDING
PORT16	10	128	FORWARDING
PORT17	10	128	FORWARDING
PORT18	10	128	FORWARDING
PORT19	10	128	FORWARDING
PORT20	10	128	FORWARDING
PORT21	10	128	FORWARDING
PORT22	10	128	FORWARDING
PORT23	10	128	FORWARDING
PORT24	10	128	FORWARDING
MOD_1	4	128	FORWARDING
MOD_2	4	128	FORWARDING

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a value from 1 to 65535.
Max Age	You can change Max. Age value, the number of seconds a bridge waits without receiving Spanning Tree Protocol configuration messages before attempting a reconfiguration. Enter a time in seconds from 6 to 40.
Hello Time	You can change the Hello time value, the number of seconds between the transmissions of Spanning Tree Protocol configuration messages. Enter a time in seconds from 1 to 10.

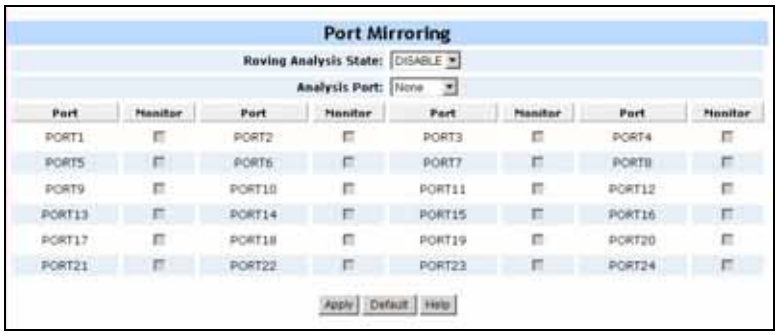
Forward Delay time	You can change forward delay time, The number of seconds a port waits before changing from its Spanning Tree Protocol learning and listening states to the forwarding status. Enter a time in seconds from 4 to 30.

2. From the Spanning Tree Configuration Menu, click **PerPort Configuration** to configure STP parameters on each port, click on the “Apply” button to set it.



Parameter	Description
Port Priority	You can make the port more or less likely in becoming the root port. The range is between 0-255. Its default setting is 128. The lowest number has the highest priority.
Path Cost	Specifies the path cost of the port. The Switch uses this to determine which port are the forwarding ports. The lowest numbers assigned are the forwarding ports. The range is between 1 and 65535 and the default value base on IEEE802.1d are: 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10

2-6-11. Port Mirroring


Port Mirroring
Roving Analysis State: DISABLE
Analysis Port: None
Port Monitor Port Monitor Port Monitor Port Monitor
PORT1 PORT2 PORT3 PORT4
PORT5 PORT6 PORT7 PORT8
PORT9 PORT10 PORT11 PORT12
PORT13 PORT14 PORT15 PORT16
PORT17 PORT18 PORT19 PORT20
PORT21 PORT22 PORT23 PORT24
Apply Default Help

Port Mirroring is a method to monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic going in or out monitored ports will be duplicated to a mirror port.

Roving Analysis State: Roving analysis is the mirroring of Fast Ethernet port traffic to another port of the same media type within a system that has an RMON probe or analyzer attached. This port allows external RMON probes (network analyzers) to monitor traffic on any switched segment.

You can monitor a designated roving analysis port to: Analyze traffic loads on each segment so that you can continually optimize your network loads by moving network segments, or troubleshoot switched network problems (for example, to find out why a particular segment has so much traffic)

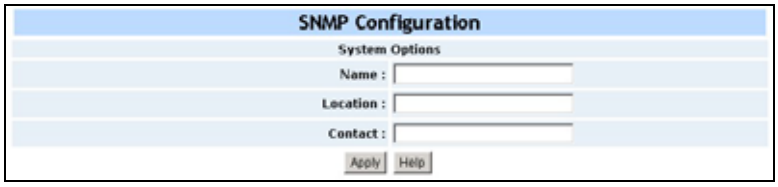
Analysis Port: You can have as many as 16 network analyzers connected to a system. For more accurate analysis, attach the analyzer to a dedicated port instead of through a repeater. When the analyzer port is set, it cannot receive or transmit any other data. Instead, it receives only the data from the ports to be monitored.

Monitor Port: The ports you want to monitor. All monitor port traffic will be copied to mirror port. You can select max 25 monitor ports in the Switch. User can choose which port that they want to monitor in only one mirror mode. For each port 1-24 you wish to monitor, click the check box next to the port. When finished, click “Apply.”

2-6-12. SNMP

Any network management platform running the Simple Network Management Protocol (SNMP) can manage the Switch provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a protocol that governs the transfer of information between management station and agent.

1. **System Options**: Use this page to define management stations as trap managers and to enter SNMP community strings. User can also define a name, location, and contact person for the switch. Fill in the system options data, and then click Apply to update the changes on this page.

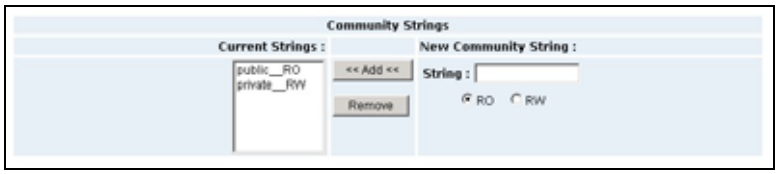


Name: Enter a name to be used for the Switch.
Location: Enter the location of the Switch.
Contact: Enter the name of a person or organization.

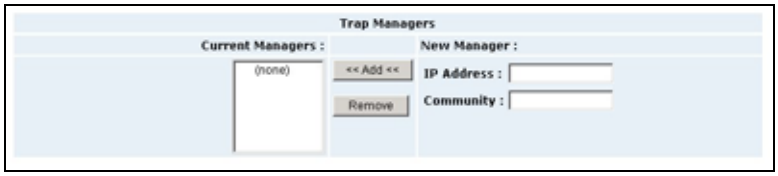
2. **Community strings**: serve as passwords and can be entered as one of the following:
   RO: Read only. Enables requests accompanied by this string to display

MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.



3. Trap Manager: The trap manager is a management station that receives traps, the system alerts generated by the Switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string the press "<<Add<<".



2-6-13. Security Manager

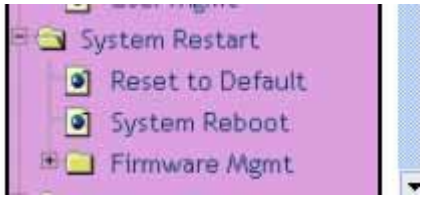
In this page, a user can change web management user name and password.

1. User name: Type the new user name.
2. Password: Type the new password.
3. Reconfirm password: Retype the new password.
4. Click "Apply."

2-6-14. TFTP Update Firmware

The following menu options provide some system control functions to allow a user to update firmware and remote boot switch system:

1. Install and run TFTP program (for example Turbo98) to the computer which is connected to the switch.
2. Copy updated firmware image **bin** into TFTP servers (Turbo98) directory.
3. Identify the IP address of the PC running the TFTP.
4. From the Main Menu, select System Restart, then Firmware Mgmt (shown in screen below). Then select TFTP Update Firmware.



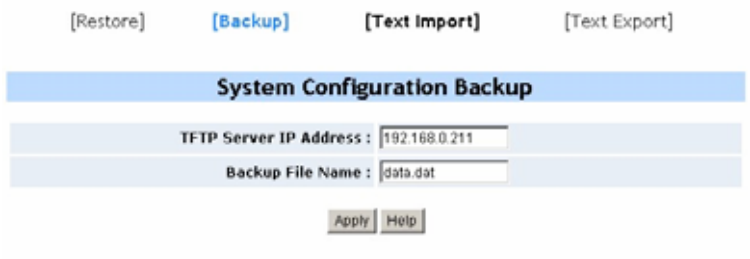
5. Enter the computers IP address into the “TFPT Server IP Address” Field
6. Type in the Firmware File Name.
7. Press Apply.

8. System will respond with “Image download completed. Would you like to update firmware” (Screen shown below)
9. To update new bin image file, press <update firmware>.
10. After update is complete, press <reboot> to restart the switch.

2-6-15. Configuration Backup

2-6-15-1. TFTP Backup Configuration

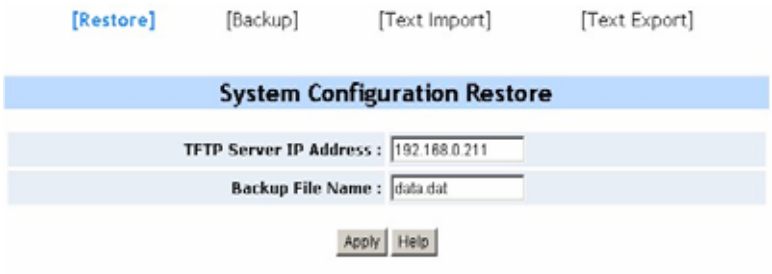
You can back up the switch system configuration in a data file, and place it on onto the TFTP server. The system configuration is saved in a binary *.dat file (example shown below is data.dat). To save the configuration file, use the page shown below to set TFTP server IP address. You can save current EEPROM value from here, then go to the TFTP restore configuration page to restore the EEPROM value.



Note: the address and file name in the above screen shot are examples

2-6-15-2. TFTP Restore Configuration

Use this page to set TFTP server address. You can restore EEPROM value from here, but you must put back image in TFTP server, Switch will download back flash image.



2-6-15-3. TFTP Import Text Configuration File

In the previous section, *TFTP Restore Configuration and TFTP Backup Configuration*, you learned how to restore and backup configuration images saved from the EEPROM and to a TFTP server. But the data in that configuration file was in binary format, as such cannot be read directly. However, there is a method to restore and read the configuration file in plain text format.

In sections 4-6-4 and 4-6 5 below, we describe the step by step procedure to both save and restore a flat text configuration file. But first, let's mention a few important points before we begin the procedure.

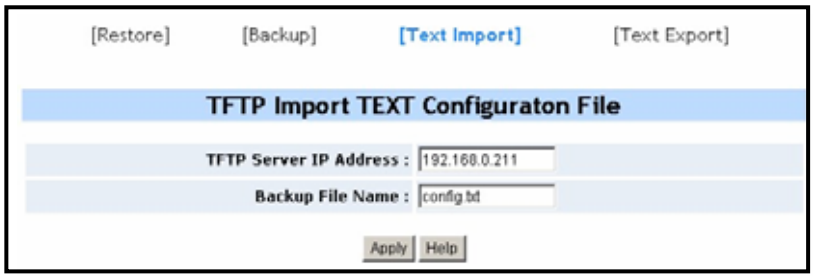
Saving and Importing text configuration files is similar to saving EEPROM images, you will also need to first set a TFTP server address and backup file name as shown in the example screens above. And like before, you will also need to place the configuration file in the TFTP server. The Switch will then be able to download the configuration data into the EEPROM as an executing batch command. You can easily duplicate switch configurations from switch to switch by simply downloading the same configuration data for each switch you like. If there are any changes you wish to make for any particular switch, you could modify the downloaded configuration file by any popularly used text editor, and then restore it to the switch.

Note: It is strongly *suggested that you use a flat text editor such as Notepad for editing the configuration file. Reason being, that some word processors tend to add unnecessary control or format codes to the text file, possibly corrupting the integrity of the file causing a file import failure.*

For every file import/export event, a status report is automatically created. The report is located in the file named 'Report.txt' located in your TFTP

server. Should there be any errors during the configuration file import, you will see details in the Report.txt file. The information in the report will give you some clues about the process and if any errors occurred.

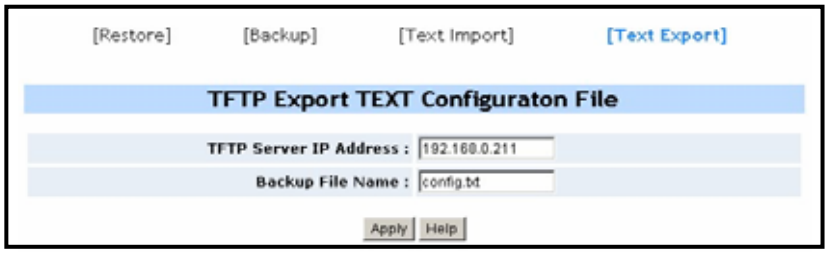
An example of a typical configuration file, and the information it contains, is showed in Appendix D at the end of this section.



Note: the address and file name on above screen shot are examples

2-6-15-4. TFTP Export Text Configuration File

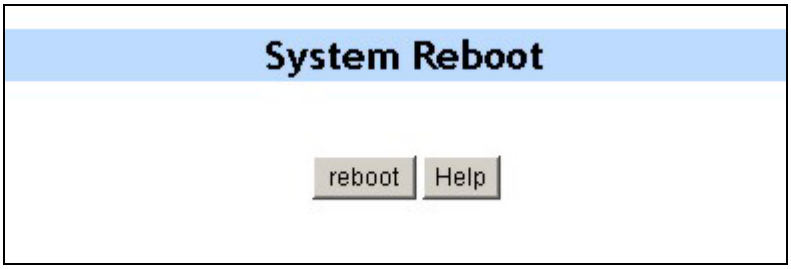
Use this page to set TFTP server IP address. You can save current EEPROM values here, and then go to the TFTP Import Text Configuration File page to restore the EEPROM value. In the following example, the backup text file is *config.txt*. It is in plain text format and can be edited by any text editor.



Note: the address and file name on above screen shot are examples

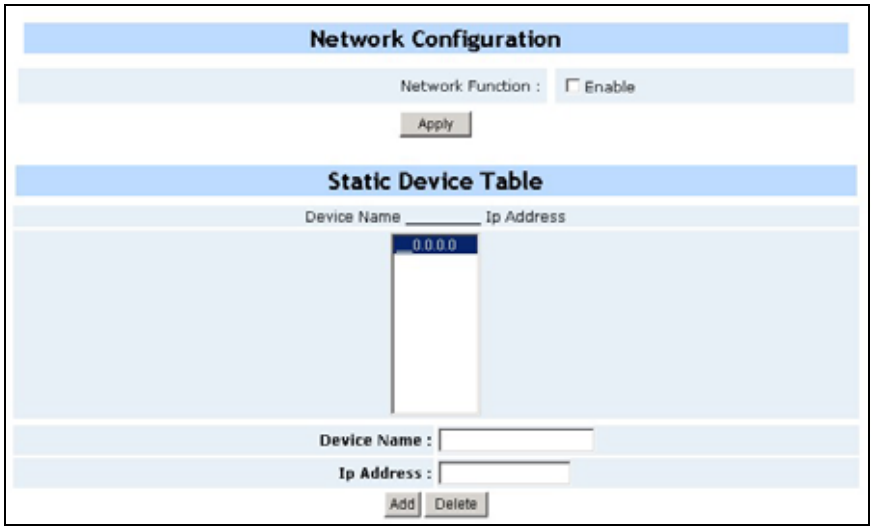
2-6-16. Reboot

Reboot the Switch with a software reset.



2-6-17. Network Tree

The “web cluster” feature will search switch nodes connected to the local network, and allows users to add/delete any network node(s) to/from the network tree. So that users not only have a network view, but also access or control switches or nodes from the local switch’s web interface. See the following diagram.



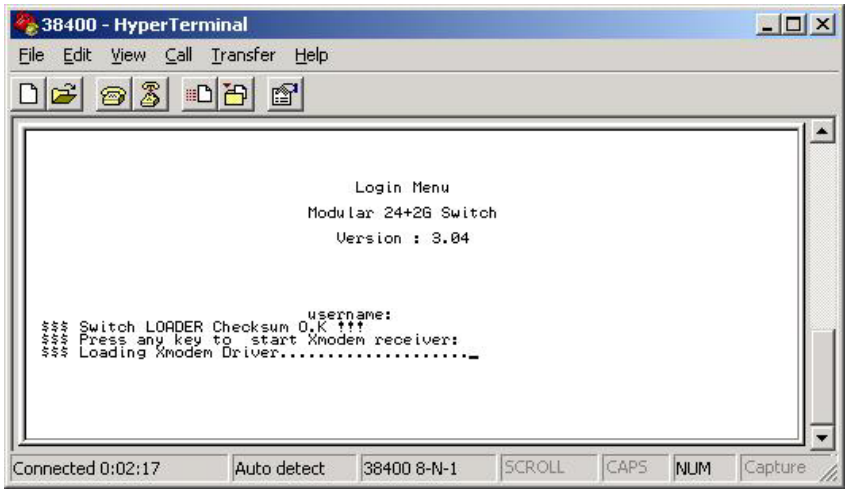
3 Console Xmodem - Update Firmware

The Switch provides a 1K Xmodem to update firmware via console. The application only works in 38400bps mode. There are two cases whereby the 1K Xmodem is used:

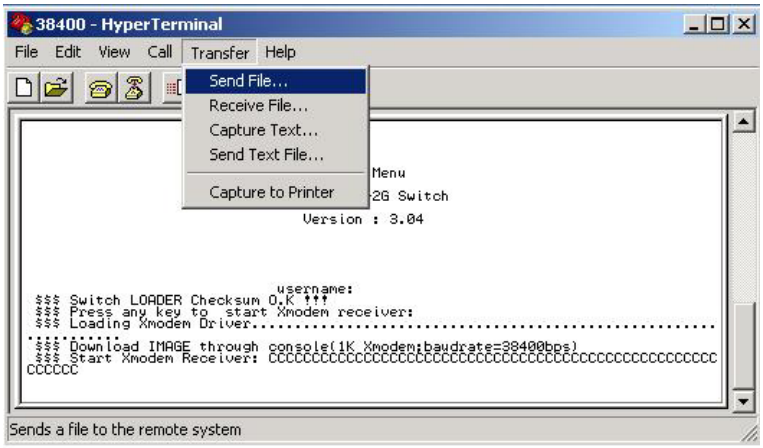
Case A. User enters "1K Xmodem receiver mode" through pressing any key within 3 seconds after system is powered on.

Case B. The system automatically enters "1K Xmodem receiver mode" if it detects the firmware checksum fail while booting.

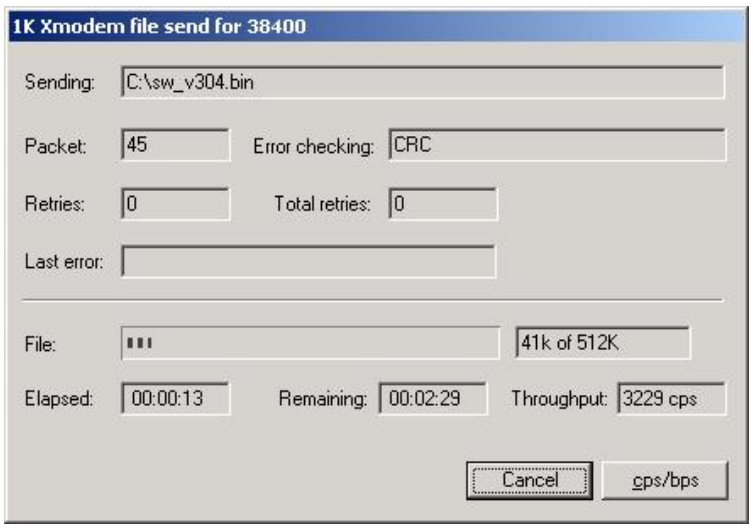
1. Start Xmodem receiver mode. Follow the screen cues by clicking any key.



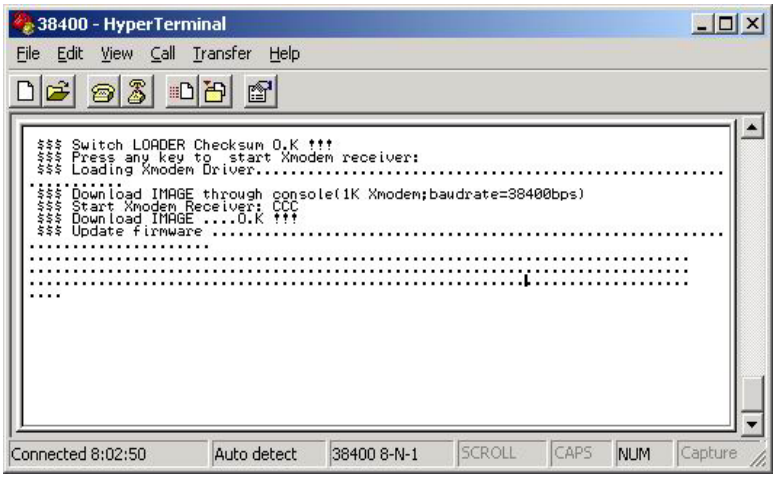
By clicking on the connected button, you will see “CCCC…”displayed on console. Select ***Transfer -> Send File.***


38400 - HyperTerminal
File Edit View Call Transfer Help
Send File...
Receive File...
Capture Text...
Send Text File...
Capture to Printer
Menu
2G Switch
Version : 3.04
username:
$$$ Switch LOADER Checksum O.K !!!
$$$ Press any key to start Xmodem receiver:
$$$ Loading Xmodem Driver.....
$$$ Download IMAGE through console(1K Xmodem;baudrate=38400bps)
$$$ Start Xmodem Receiver: CCCC

4. Start download image file.



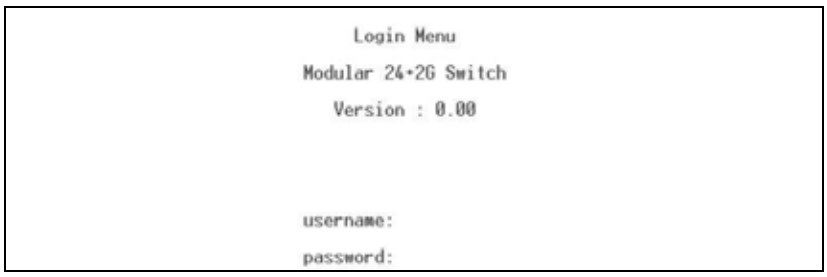
5. Finish downloading the image - the Switch system will update firmware automatic. Update firmware ok - the Switch will reboot.



4 Console Menu Line

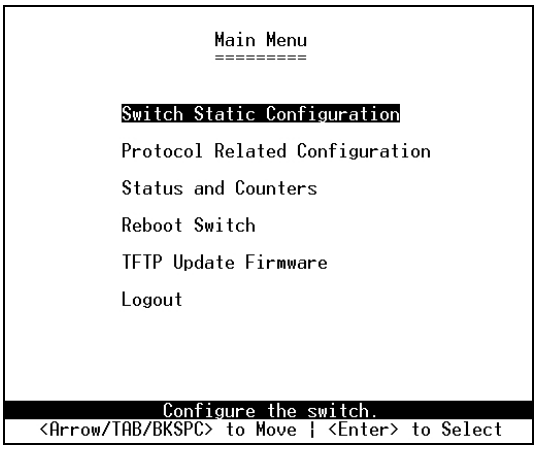
Being SNMP manageable, The Switch features a serial interface to manage and to monitor the system. Attach a VT100 compatible terminal or a PC running a terminal emulation program (i.e. HyperTerminal) to the serial port on the switch's front panel. A user can follow the Console menu to manage and control the Switch.

You can type user name and password to login. The default user name is "admin", with **no** default password.



4-1. Main Menu

There are six items on the Main Menu page. They are as follows:



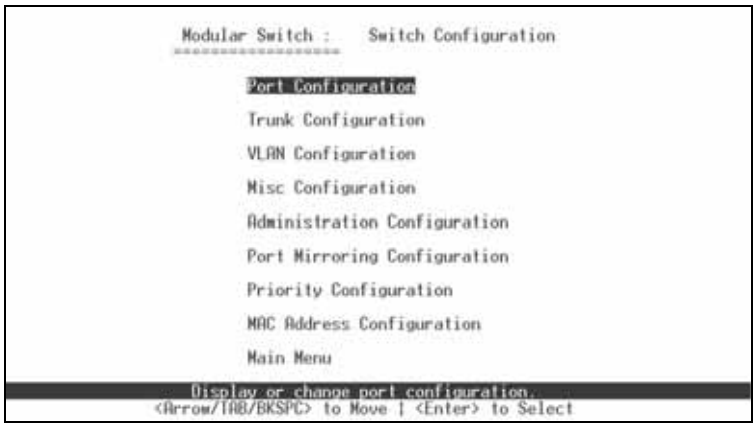
Switch Static Configuration:	Configure the Switch.
Protocol Related Configuration:	Configure the protocol function.
Status and Counters:	Show the status of the Switch.
Reboot Switch:	Restart the system or reset Switch to default configuration.
TFTP Update Firmware:	Use tftp to download image.
Logout:	Exit the menu line program.

<Control Key>

The control key provided in all menus as follow:

Tab:	Move the cursor to next item.
Backspace:	Move the cursor to previous item.
Enter:	Select item.
Space:	Toggle selectable items

4-2. Switch Static Configurations



From the Switch Configuration page, users can alter Port, Trunk, VLAN, Administrative, Port Mirroring, Priority, MAC address and Miscellaneous configurations. The following sections in this manual go over each configuration in detail.

The following action menu line is provided within the configuration pages.

<Quit>: Exit the current page and return to previous menu.

<Edit>: Configure items. When finished with setting configurations, press **Ctrl+A** to go back action menu line.

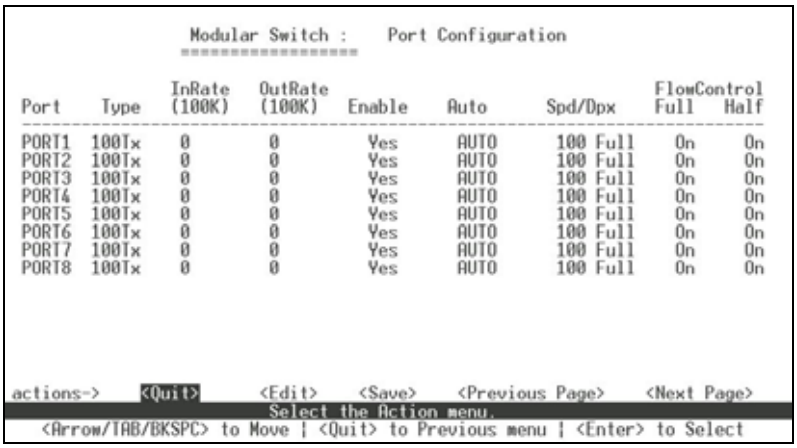
<Save>: Save all configured values.

<Previous Page>: Return to previous page.

<Next page>: Go to next page.

4-2-1. Port Configuration

This screen allows the configuration of each port. Press **<Space>** key to change the status of each item.



InRate (100Kbps/unit): Here the user can set input rate control. Each unit is 100K. The valid range is 0~1000.
0: disable rate control.
1~1000: valid rate value.

OutRate (100Kbps/unit): User can set output rate control. Each unit is 100K. The valid range is 0~1000.
0: disable rate control.
1~1000: valid rate value.

Enabled: User can disable or enable each port. “Yes” means that the port is enabled. “No” means the port is disabled.

Auto: User can set the auto-negotiation mode.

a. Force - specify the speed/duplex on this port
b. NWay Force - specify the speed/duplex on this port with auto-negotiation enabled.
c. Auto – for the Switch to automatically determine the highest speed and duplex mode possible

Spd/Dpx: User can set 100Mbps or 10Mbps speed on port 1~port 24 (depending on the performance of the uplink module card), 1000Mbps on port25~port26, and set full duplex or half-duplex modes.

Flow Control:
Full: User can enable or disable full flow control function (pause)
Half: User can enable or disable half flow control function (backpressure).

NOTE:

1. **Selecting <Save> will only save the new configuration on the current page.**
2. **If any static trunk groups exist (e.g. TRK1, TRK2…) they will be sorted to the bottom of the displayed list, below the ports.**

4-2-2. Port Abnormal Traffic Detection

The Abnormal Traffic Detection function allows the user to configure the bandwidth threshold up to which the specified ports can receive broadcast packets. If the incoming broadcast packets exceed this limit, the Switch can disable that port for a specified time or permanently (‘forever’).

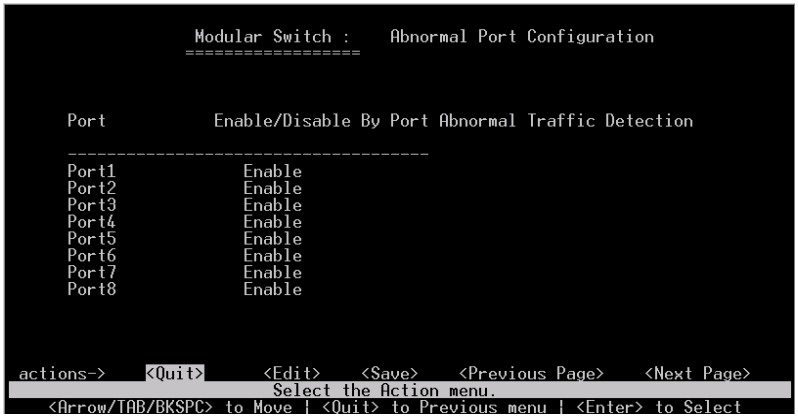
Modular Switch : Abnormal Traffic Detection Configuration
Port Abnormal Traffic Detection Enable
Port Abnormal Traffic Detection Configuration
Port Abnormal Traffic Detection Port Configuration
Previous Menu
Enable port Abnormal Traffic Detection.

Select the menu “Port Abnormal Traffic Detection Enable” to enable or disable the function. The menu “Port Abnormal Traffic Detection Configuration” is for configuration management of the broadcast packet detection and the processing afterwards. The menu “Port Abnormal Traffic Detection Port Configuration” is for enabling or disabling the function per port.

Modular Switch : Port Abnormal Traffic Detection Enabled
Port Abnormal Traffic Detection:Disabled
actions-> <Edit> <Save> <Quit>
Select the action menu.
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select

This is for enabling or disabling the function for the whole switch.

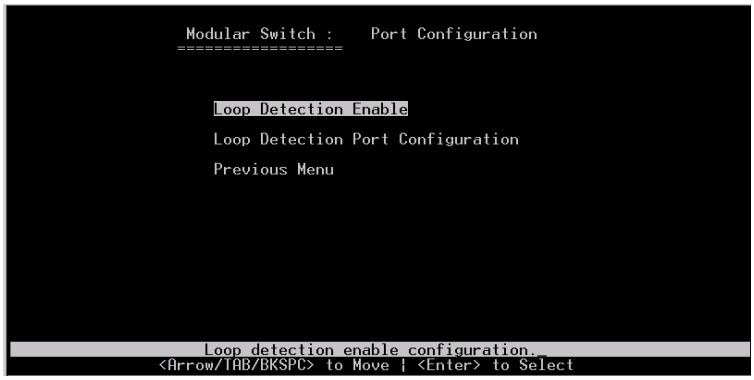
Attribute	Meaning
Port Traffic Detection Enable (previous screen)	“Enable” or “Disable” this function
Port Packet Limit	The bandwidth threshold for incoming broadcast packets
Port Protection Interval Forever	Enable: Disable the port forever if the incoming broadcast packets exceed the bandwidth threshold continuously in the specified monitor time interval. Disable: Disable the port only for a specified time interval if the incoming broadcast packets exceed the bandwidth threshold continuously in the specified monitor time interval
Port Protection Interval	The time period that the port will be disabled if the incoming broadcast packets exceed the bandwidth limit
Port Protection Monitor Times	The period over which a port must experience an overflow of broadcast packets before being disabled
Port / Protection (next screen)	Enable or Disable the Abnormal Traffic Detection function per port



This screen is for enabling or disabling the function per port.

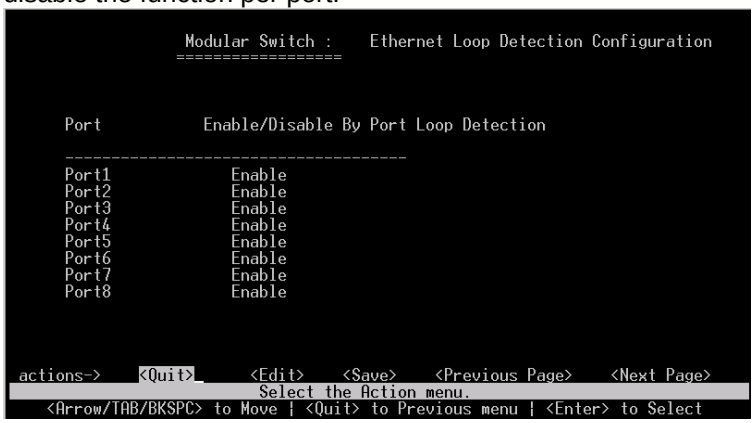
4-2-3. Ethernet Loop Detection

The Ethernet Loop Detection function provides a means to detect the loop condition on the sub-network connected to the port. If such condition is detected, the port will be disabled by the Switch.



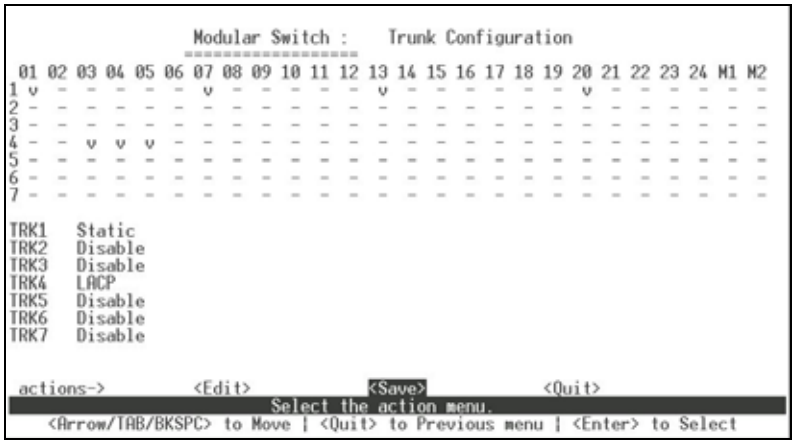
Select the menu “Loop Detection Enable” to enable or disable the function for the whole Switch.

Select the menu “Ethernet Loop Detection Configuration” to enable or disable the function per port.



4-2-4. Trunk Configurations

Use the Trunk Configuration page shown below to create trunk groups. The Switch supports a maximum of seven trunk groups. Each trunk group may be comprised of up to four ports, selected from any of the range of ports 1~24, M1 and M2.



Create a trunk group

1. Select **<Edit>** on the “actions” menu

2. The numbers 1-7 running down the left side of the page represent the maximum allowable (7) trunk groups. Use the Arrow/TAB/Backspace keys to navigate through these fields. Press the <**space>** key to add a port to a trunk group (represented by a ‘v’).

3. Below the port group identifiers are TRK1~TRK7, representing the maximum (7) trunk groups, and next to each is a status indicator.

   Static – A standard port-based (non-LACP) trunk.
   LACP - Trunking with Link Aggregation Control Protocol.
   Disable - The trunk group is disabled.

   Set each trunk to; Static, LACP, or disabled as desired.

4. Press Ctrl+A to return to the action menu line. Select <Save> to save all configured values.

NOTE: **Since all ports in the same static trunk group behave as a single port, changes to the Port Configurations for a trunk will apply to all members of the trunk simultaneously.**

4-2-5. VLAN Configuration

Use the VLAN Configuration page (shown below) to set port-based VLAN or 802.1q VLAN or to deactivate the VLAN function. There are a few configuration examples in Appendix B for your reference.

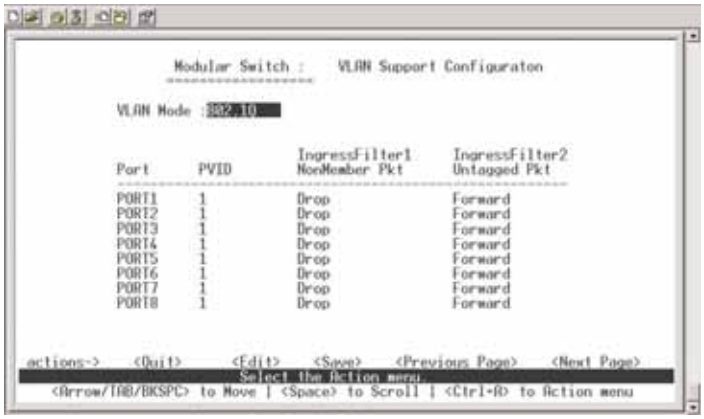
NOTE: Each time the VLANs are modified, the Switch should be restarted to assure that the new configurations take affect.

There are three types to select:

a. Disable (VLAN)
b. Port-based
c. 802.1q (Tag-based)

To enable or disable VLAN Support, enter the VLAN Support Configuration screen shown below. The default configuration VLAN Mode for the Switch is “Disabled”.

If 802.1q VLAN is set, you can set PVID, ingress filtering 1 and ingress filtering 2 on the VLAN Support Configuration page.



1. **PVID (Port VID : 1~4095):** Select the PVID. Each port allows the user to set one PVID, the range is 1~4095, the default PVID is 1. Multiple ports can share the same PVID, but in the same switch all the PVIDs of the switch's ports must belong to the same 256-number segment, for example 1~255 or 256~511 or …3840~4095.

2. **NonMember Pkt:** This matches Ingress Filtering Rule 1 in web-based management (p.33).
   Either forward only packets with a VID that matches this port's

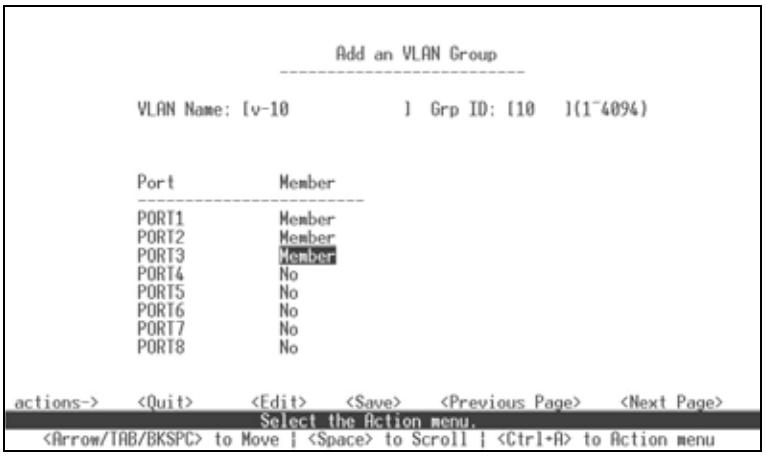
configured VID, or drop the frame when a VID is not matching this port's configured VID. Press <**Space>** to choose 'drop' or 'forward'. The default is 'drop'. This is the same as filtering rule 1 'enabled' in web-based management (p.33).

3. **UnTagged Pkt:** This matches Ingress Filtering Rule 2 in web-based management (p.33).
   Either drop or forward untagged frames. Press <**Space>** to choose 'drop' or 'forward'. The default is '**forward'**. This is the same as filtering rule 2 'enabled' in web-based management (p.33).

4-2-5-1. Create a VLAN Group

Create Port-Based VLAN

To create a port-based VLAN and to add member/non-member ports to it.



1. Select **<Edit>.**

2. **VLAN Name:** Type a name for the new VLAN.

3. **Grp ID:** Type the VLAN group ID. The group ID range is 1~4094.

4. **Member:** Press <**Space>** key to choose VLAN member. There are two types to select:

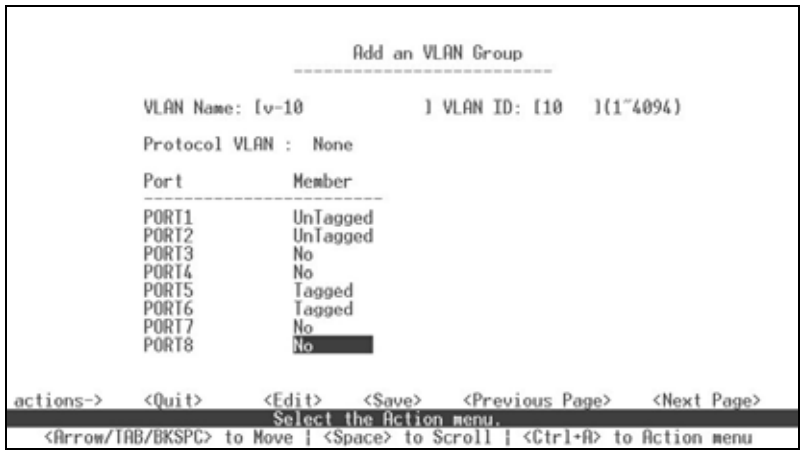
1. Member: The port is a member of the current VLAN.
2. NO: The port is NOT a member of the current VLAN.

5. Press **Ctrl+A** to go back to the action menu line.

6. Select **<Save>** to save all configure values.

NOTE: **If the trunk groups exists (e.g. TRK1, TRK2…) you can see it sorted in the list below the ports. Remember, trunks can be assigned to members of a VLAN just as ports can.**

Create an 802.1q (tag-based) VLAN



To create an 802.1q VLAN and add tagged /untagged member ports to it, follow the procedure below.

1. Select **<Edit>**.

2. **VLAN Name:** Type a name for the new VLAN.

3. **VLAN ID:** Type a VID (between 2~4094). The default is **1**. There are 256 VLAN groups provided for configuration. Each port can join more than one, (up to 256) tagged VLAN groups.

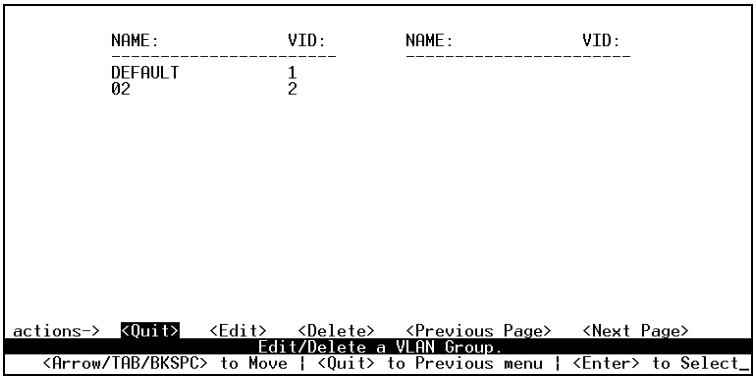
4. **Protocol VLAN:** Press <**Space**> key to choose protocol type. If you are not applying protocol VLAN, you must set the value to “None”. You can not set a port to join more than one VLAN/VID with the same protocol.

5. **Member:** Press <**Space**> key to choose VLAN member. There are three types to select from:

    a. **UnTagged**: this port is a member port of this VLAN group and outgoing frames are NOT VLAN-Tagged frames.
    b. **Tagged**: this port is a member port of this VLAN group and outgoing frames are VLAN-Tagged frames.
    c. **No**: the port is NOT a member port of this VLAN group.

6. Press **Ctrl+A** to go back to the action menu line.
7. Select **<Save>** to save all configure values.

4-2-5-2. Edit / Delete A VLAN Group

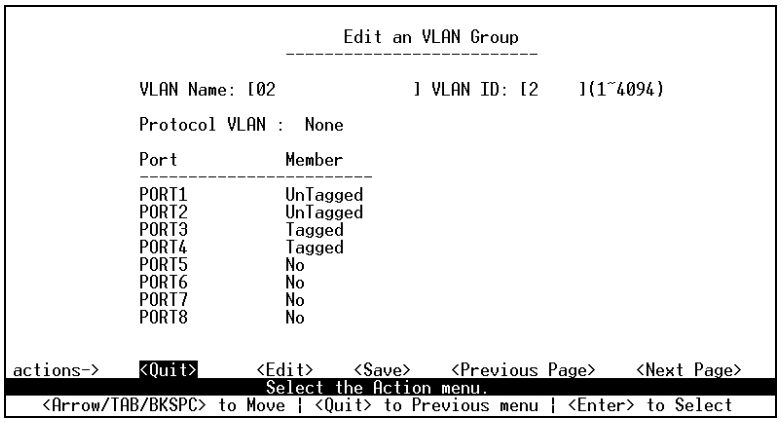


Use this page to edit or delete a VLAN group.

1. Select **<Edit> or <Delete>** item.
2. Choose the VLAN group that you want to edit or delete and then press enter.
3. A user can modify the protocol VLAN item and whether the member port is tagged or un-tagged, and remove some member ports from an existing VLAN group.

4. After editing the VLAN, press the **<Save>** key to save all configured values.

NOTE:
1. **Pressing <Enter> once will complete deletion on delete mode.**
2. **The VLAN Name and VLAN ID cannot be modified.**
3. **The default VLAN cannot be deleted.**



4-2-5-3. Groups Sort Mode

In this page, a user can select VLAN group sort mode. The options are:
(1) sorted by name
(2) sorted by VID

In the *Edit/Delete a VLAN group* page, the following page will be displayed:

In the *Edit/Delete a VLAN Group* page, the result of the sorting process will be displayed.

NAME:	VID:	NAME:	VID:
DEFAULT	1		
A1	3		
B4	4		
V2	2		

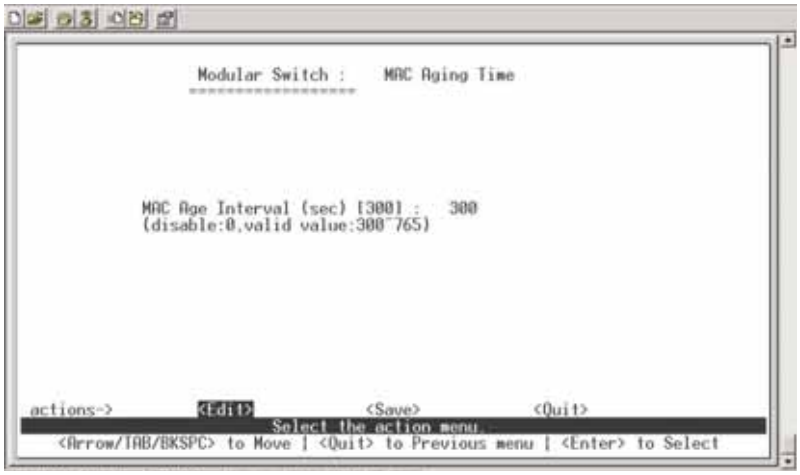
In the *Edit/Delete a VLAN Group* page, the result of sorting by VID is displayed.

NAME:	VID:	NAME:	VID:
DEFAULT	1		
V2	2		
A1	3		
B4	4		

4-2-6. Misc. Configuration

4-2-6-1. MAC Age Interval

In the MAC Aging Time page, a user can adjust the time a MAC address remains valid. Type the number of seconds that an inactive MAC address remains in the Switch's address table. The valid range is 300~765 seconds. The default is 300 seconds.



4-2-6-2. Broadcast Storm Filtering

Use the Broadcast Storm Filter Mode page to configure broadcast storm control.

1. Select **<Edit>** to configure the broadcast storm filter mode.

2. Press <**Space>** key to choose the threshold value.
   The valid threshold values are 5%, 10%, 15%, 20%, 25% and NO. Selecting a NO threshold effectively turns off broadcast storm.

4-2-6-3. Max Bridge Transmit Delay Bound

1. **Max bridge transmit delay bound:** Limit the packets queuing time in the Switch. If enabled, the packets queued that exceed this time frame will be dropped. Press <**Space>** key to set the time. The valid values are 1sec, 2secs, 4secs, and OFF. The default is OFF.

2. **Low Queue Delay Bound:** Limits the low priority packets queuing time in the Switch. When enabled, the low priority packets in the Switch that have exceeded the Low Queue Max Delay Time it will be sent. Press <**Space>** key to enable or disable this function.

3. **Low Queue Max Delay Time:** To set the time that low priority packets are queued in the Switch. Default Max Delay Time is 255ms. The valid range is 1~255 ms.

NOTE: Make sure that the "Max bridge transit delay bound control" is enabled before the "Low Queue Delay Bound" is enabled because the former must be activated before the latter in order for Bridge Transit Delay Bound to function properly.

4-2-6-4. Port Security

A port in security mode will be "locked" and does not permit address learning. Only incoming packets with Static Media Access Control (SMAC) already existing in the address table can be forwarded normally. The user can disable the port from learning any new MAC addresses, then use the static MAC address screen to define a list of MAC addresses that can use the secured port.

To enable/disable Port Security

1. Select **<Edit>**.
2. Press **Space** key to choose enable / disable item.
3. Press **Ctrl+A** to go back action menu line.
4. Select **<Save>** to save all configure value.
5. You can press **<Next Page>** to configure port9 ~ port26, press **<Previous Page>** return to last page.

4-2-6-5. Collisions Retry Forever

Collisions Retry Forever:

Disabled – In half-duplex, if collisions occur, the Switch will retry sending the frame 48 times before the frame is dropped.

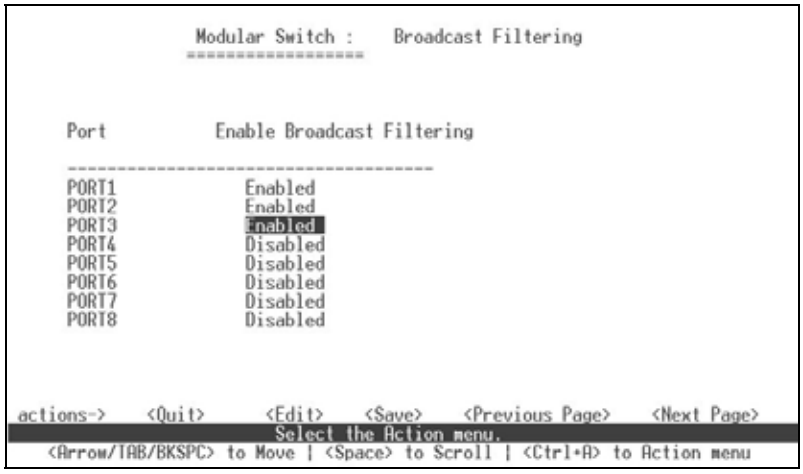
Enabled – In half-duplex, if collisions occur, the Switch will retry sending the frame indefinitely.

4-2-6-6. Hash Algorithm

CRC-hash/Direct-map Hash Algorithm.

4-2-6-7. Broadcast Filtering

In a typical LAN network, there are substantial amounts broadcasted traffic. In order to filter the broadcast traffic, the user may disable or enable Broadcast Filtering for each port.

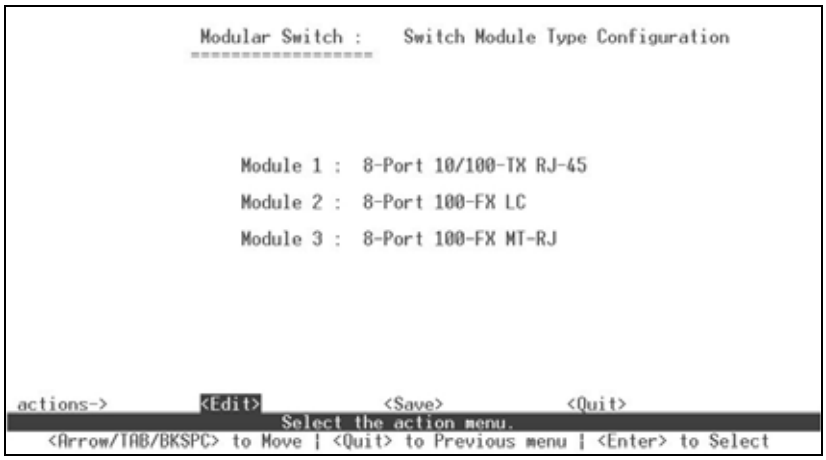


4-2-6-8. Module Type Configuration

Selection of the physical Module Type for the Switch.

Support module type：

1. No Module
2. 8-Port 10/100 Base-TX RJ-45
3. 4-Port 100 Base-FX ST/SC
4. 8-Port 100 Base-FX LC
5. 8-Port 100 Base-FX MT-RJ
6. 8-Port 100 Base-FX BiDi



4-2-7. Administration Configuration

4-2-7-1. Change Username

Use UserName Configuration page to change administrator's user name. Type the new user name, then select **<Save>** to change the username.

4-2-7-2. Change Password

Use Password Configuration page to change administrator's login password.

4-2-7-3. Device Information

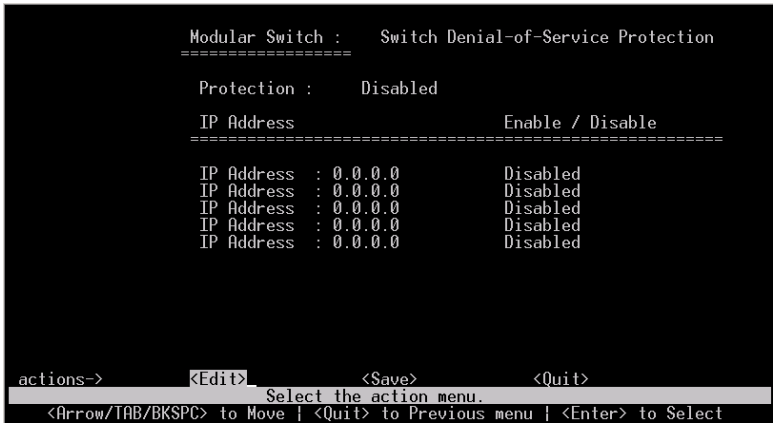
Use Device Information page to configure the device Name, Description, Location, and port content information.

4-2-7-4. IP Configuration

Use IP Configuration page to configure the IP settings and Gateway settings, and DHCP enable/disable.

4-2-7-5. Switch Denial-of-Service Protection

The Switch can be protected from denial-of-service attacks. If the user specifies all the IP addresses from which the Switch can be managed, the Switch will discard all management packets from other sources.



The function can be enabled or disabled. The specified enabled IP addresses will be granted management rights.

4-2-7-6. Network Configuration

Use the Network Configuration page to Enable/Disable (Toggle disable/enable) the Network Device Auto-Discovery feature.

4-2-7-7. Add Static Network Device

Add, edit, and configure static network devices from the Add Static

Network Device page.

4-2-8. Port Mirroring Configuration

Port mirroring is a method for monitoring traffic in switched networks. Traffic passing through ports can be monitored by one specific port. That is the traffic going in or out of the monitored ports will be duplicated into a separate monitoring port.

Press <**Space>** key to change configuration of each item.

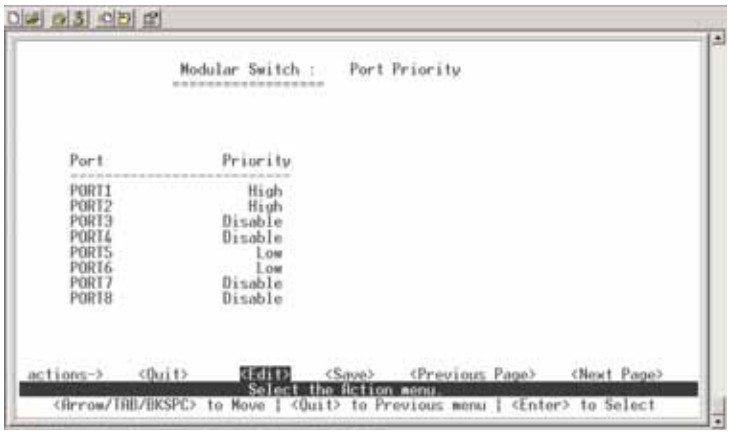
1. Select **<Edit>**
2. **Sniffer Mode:** Press <**Space**> key to select the sniffer mode. The options are: Disable / Rx / Tx / Both.
3. **Monitoring Port -** sniffer port can be used to monitor all ports traffic. Press <**Space**> key to select it.
4. **Monitored Port -** the ports you want to monitor. All monitored port traffic will be copied to the sniffer port. You can select a maximum of 25 monitored ports in the Switch. The user can choose the ports to be monitored in one sniffer mode. Press **Space** key to select the member port, "V" is a member, while "—"is not a member.
5. Press **Ctrl+A** go back to the action menu line
6. Select **<Save>** to save all configured values.
7. On the action menu line you can press **<Next Page>** to configure port9 ~ port26, select **<Previous Page>** return to last page.

NOTE: Only one sniffer mode can be activated at a time.

4-2-9. Priority Configuration

4-2-9-1. Port Static Priority

The static priority is port-based. When a port is assigned with a high priority, all incoming packets to this port also always have a high priority.



4-2-9-2. 802.1p Priority Configuration

There are 0~7 priority queue levels that can be assigned.

1. Select **<Edit>**
2. Press <**Space**> key to select the priority level mapping from low to high queue.
3. **High/Low Queue Service Ratio H:L -** User can select the ratio of high priority packets and low priority packets.
4. Press **Ctrl+A** go back action menu line.
5. Select **<Save>** to save all configure value.

4-2-10. MAC Address Configuration

4-2-10-1. Static MAC Address

When you add a devices static MAC address to the switch MAC address table, it will remain in the Switch's address table regardless of whether the device is physically connected to the Switch or not. This saves the Switch from having to re-learn a device's MAC address when the Switch is disconnected or powered-off.

In the Static MAC Address Configuration page, the user can add / modify / delete a static MAC address.

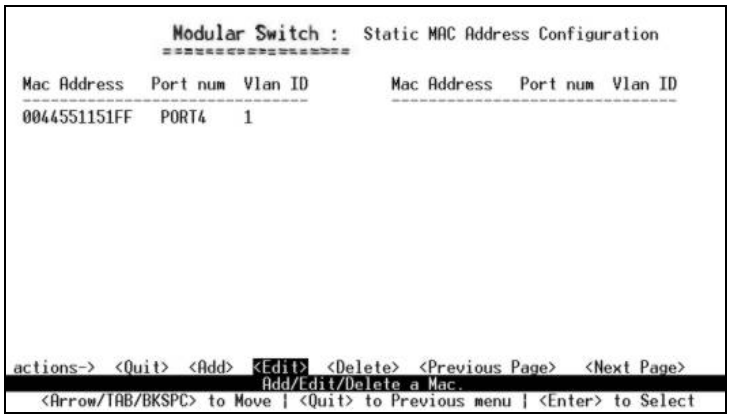
Add static MAC address

1. Select **<Add>** and then **<Edit>** to add static MAC address.
2. **MAC Address -** Enter the MAC address to the port that should permanently forward traffic regardless of the Switch's network activity.
3. **Port num -** press **<Space>** key to select the port number.
4. **Vlan ID -** If they are tag-based (802.1q), VLANs are set up on the Switch. Static addresses are associated with individual VLANs. Type the VID to associated with the MAC address.
5. Press **Ctrl+A** to go back to the action menu line, and then select **<Save>** to save all configured values.

Edit static MAC address

1. Press **<Edit>** key.

2. Choose the MAC address that you want to modify and then press Enter.



3. Press **<Edit>** key to modify all the items.

4. Press **Ctrl+A** to go back to the action menu line, and then select **<Save>** to save all configured values.

Delete static MAC address

1. Press **<Delete>** key.
2. Choose the MAC address that you want to delete and then press enter.
3. By pressing **<Enter>** once will complete the deletion.

4-2-10-2. Filtering MAC Address

MAC address filtering allows the Switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. In this page, the user can

add / modify / delete filter MAC address.

Add filter MAC address

1. Select **<Add>** and then **<Edit>** to add a filter MAC address.
2. **MAC Address:** Type the MAC address to be filtered.
3. **Vlan ID:** If they are tag-based (802.1q), VLANs are set up on the Switch. Type the VID to associate with the MAC address.
4. Press **Ctrl+A** to go back to the action menu line, and then select <Save> to save all configured values.

Edit filter MAC address

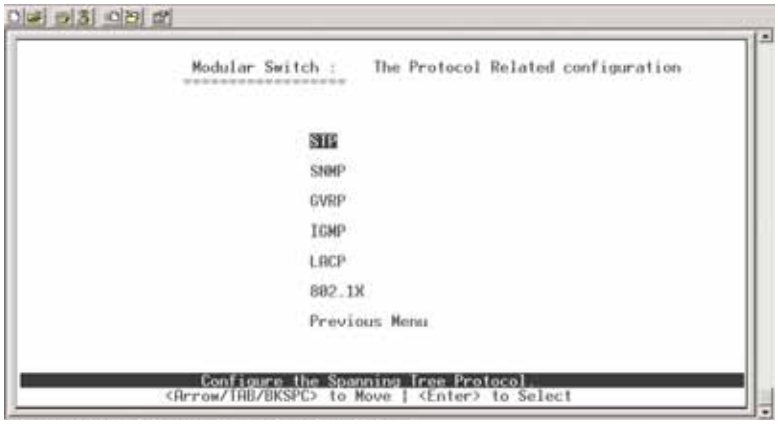
1. Press **<Edit>** key.
2. Choose the MAC address that you want to modify and then press Enter.

3. Select **<Edit>** to modify all the items.
4. Press **Ctrl+A** to go back to the action menu line, and then select **<Save>** to save all configured values.

Delete filter MAC address

1. Select **<Delete>** to delete a filter MAC address.
2. Choose the MAC address that you want to delete and then press Enter.
3. By pressing **<Enter>** once, the deletion will be completed.

4-3. Protocol Related Configuration

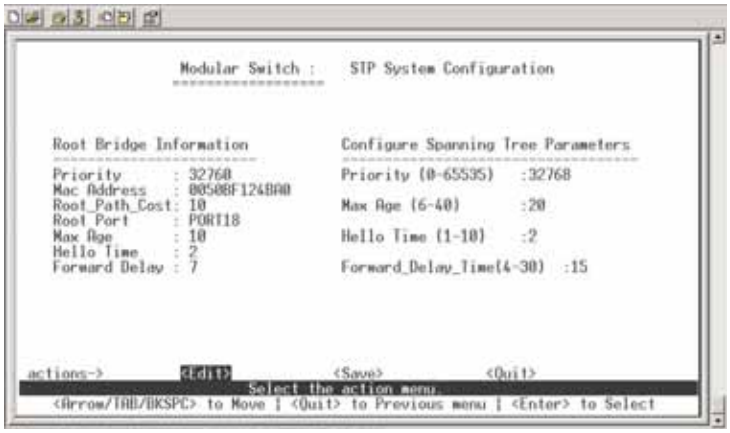


4-3-1. Spanning Tree Protocol (STP)

4-3-1-1.STP Enable

Use the STP Enabled/Disabled Configuration page to enable or disable the Spanning Tree function (STP). Press <**Space**> key to toggle enable or disable.

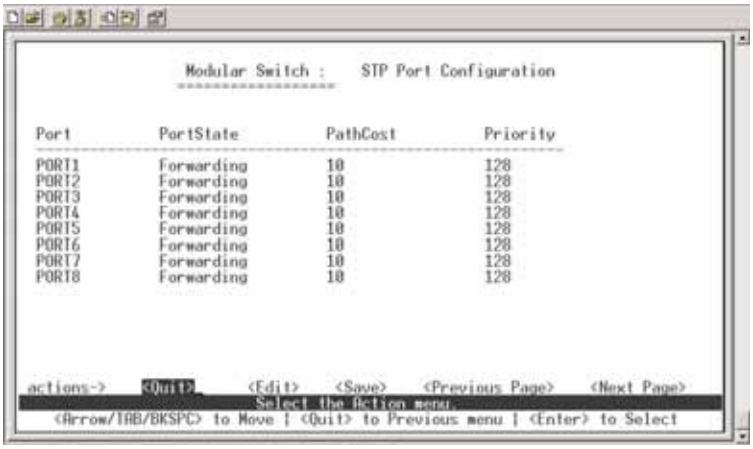
4-3-1-2. System Configuration



Editing STP Configurations

1. You can view spanning tree information (Priority, MAC Address, Root path cost, Root port, Maximum age, Hello time, and Forward delay) about the Root Bridge on the left.
2. On the right, user can set new values for selected STP parameters.

4-3-1-3. Per Port Configurations



STP modifications on a per-port basis

Select Spanning Tree Protocol parameters may be modified on a port by port basis form the STP Port Configuration screen shown above. Description of the editable parameters are as follows:

1. **PortState:** Display spanning tree status about each port whether it is forwarding or blocking.
2. Select **<Edit>**
3. **PathCost:** Specifies the path cost of the port that the Switch uses to determine which port are the forwarding ports
4. **Priority:** This means port priority, you can make it higher or lower or making it more likely to become the root port
5. Press **Ctrl+A** go back to the action menu line
6. Select **<Save>** to save all configured values
7. On the action menu line you can press **<Next Page>** to configure Port 9 ~ Port 26, press **<Previous Page>** return to last page.

4-3-2. SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Use the SNMP Configuration page to define management stations as trap managers and to enter SNMP community strings. User can also define a name, location, and contact person for the Switch.

4-3-2-1. System Options

SNMP System Options are accessible from the System Options Configuration page shown above. To set System Name, Contact and Location:

1. Press **<Edit>**.
2. **System Name:** Type a name to be used for the Switch.
3. **System Contact:** Type the name of contact person or organization.
4. **System Location:** Type the location of the Switch.
5. Press **Ctrl+A** go back action menu line.
6. Press **<Save>** to save the configured value.

4-3-2-2. Community Strings

Use the SNMP Community Configuration page to Add/ Edit/ Delete SNMP community strings.

1. **Community Name:** The name of current strings.
2. **Write Access:** Enable the rights is read only or read-write.
   Restricted: Read only, enables requests accompanied by this string to display MIB-object information.
   Unrestricted: Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.

4-3-2-3. Trap Managers

A trap manager is a management station that receives traps, a system alerts generated by the Switch. If no trap manager is defined, no traps can be issued. Create a trap manager by entering the IP address of the station and a community string from the Trap Managers Configuration page.

4-3-3.GVRP

Use the GVRP Configuration page to enable / disable the GVRP (GARP VLAN Registration Protocol) support.

1. Select **<Edit>**.
2. Press **Space** key to choose Enabled / Disabled.
3. Press **Ctrl+A** go to the action menu line.
4. Select **<Save>** to save configured values.

4-3-4. IGMP

Use the IGMP Configuration page to enable / disable the IGMP support.

1. Select **<Edit>**.
2. Press **Space** key to choose Enabled / Disabled.
3. Press **Ctrl+A** go to the action menu line.
   Select **<Save>** to save configured values.

4-3-5. LACP

Use this page to configure and view all LACP status.

4-3-5-1. Working Port Setting

Use this page to set the actual work ports in a trunk group.

1. Select **<Edit>**.
2. **Group:** Display the trunk group ID.
3. **LACP:** Display the trunk group's LACP status.
4. **LACP Work Port Num:** The maximum number of ports that can be aggregated at the same time. If it is a LACP static trunking group, the exceed ports are standby and able to aggregate if work ports fail. If it is a local static trunking group, the number must be the same as group ports.

NOTE: Before setting this page, you must first set the trunk groups on the *Trunk Configurations* page.

4-3-5-2. State Activity

User may alter the LACP Port State from the LACP Port State Active Configuration menu

1. Select **<Edit>**
2. Press the **<Space>** key to choose the item.
   Active: The port automatically sends LACP packets.
   Passive: The port does not automatically send LACP packets, and responds only if it receives LACP packets from another device

3. Press **Ctrl+A** to go to the action menu line
4. Select **<Save>** to save configured values.
   If the user set LACP mode in the trunk group, all of the member ports of this trunk group will be set to and an "Active" status automatically.

4-3-5-3. LACP Status

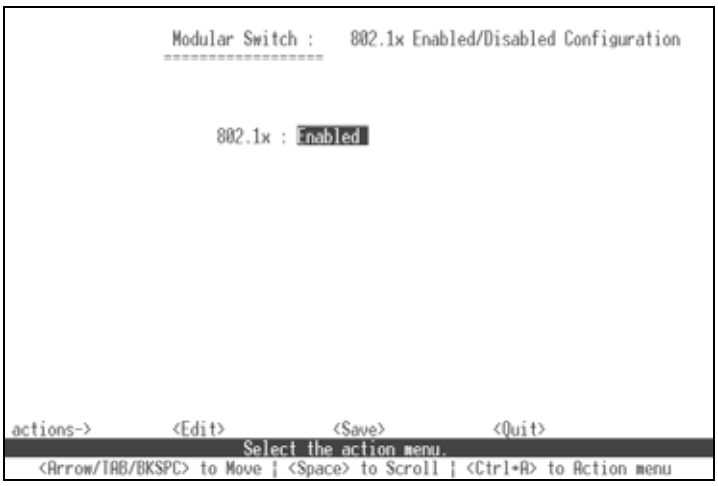
When you have set the trunking groups, go to the LACP Group Status page to see the related Static trunk group information.

<Quit>: Exit this page and return to previous menu
<Previous Page>: Return to previous page
<Next page>: Go to next page

4-3-6. 802.1x Protocol

The 802.1x protocol page allows a user to configure and view all the 802.1x status.

4-3-6-1. 802.1x Enable



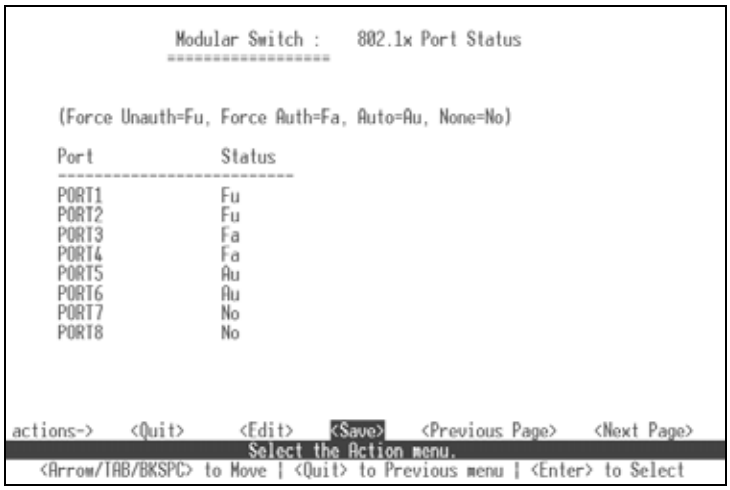
1. Select **<Edit>**.
2. Press **Space** key to choose Enabled / Disabled.
3. Press **Ctrl+A** go back action menu line.
4. Select **<Save>** to save configure value.

4-3-6-2. 802.1x System Configuration

1. Press **<Edit>**.
2. **Radius Server IP Address:** the IP address of the authentication server.
3. **Shared Key:** A key shared between the Switch and authentication server.
4. **NAS, Identifier:** A string used to identify the Switch.
5. **Server Port:** The UDP port number used by the authentication server to authenticate.
6. **Accounting Port:** The UDP port number used by the authentication server to retrieve accounting information.
7. Press **Ctrl+A** go back action menu line.
8. Press **<Save>** to save configured value.

4-3-6-3. 802.1x PerPort Configuration

In the 802.1x Port Status page, a user can set the authorization status to activate 802.1x function on a port-by-port basis.



1. Select **<Edit>**.
2. **Status:** Press **<Space>** key to choose Fu / Fa / Au / No authorization status.
3. Press **Ctrl+A** go back action menu line.
4. Select **<Save>** to save all configured value.

Fu: Force the specific port to be unauthorized.
Fa: Force the specific port to be authorized.
Au: The state of the specific port that was determined by the outcome of the authentication.
No: The specified port does not support IEEE 802.1x function.

4-3-6-4. 802.1x Miscellaneous Configuration

Miscellaneous 802.1x settings such as shown in the 802.1x Misc. Configuration page are editable as follows:

1. Press <Edit>.
2. Quiet Period: Used to define period of time during which it will not attempt to acquire a supplicant (Default time is 60 seconds).
3. Tx Period: Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
4. Supplicant Timeout: Used to determine timeout conditions in the exchange between the supplicant and authentication server (Default value is 30 seconds).
5. Server Timeout: Used to determine timeout conditions in the exchange between the authenticator and authentication server (Default value is 30 seconds).
6. ReAuthMax: Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
7. Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).
8. Press Ctrl+A go back action menu line.
9. Press <Save> to save configured value.

4-4. Status and Counters

You can press the **Tab** or **Backspace** key to access an item, and press **Enter** key to select item.

4-4-1. Port Status

The Status and Counters page displays the status of each port.

Link Status: Displays whether the port is linked or not linked.

InRate: Displays the input rate control (100K/unit) setting value.

OutRate: Displays the output rate control (100K/unit) setting value.

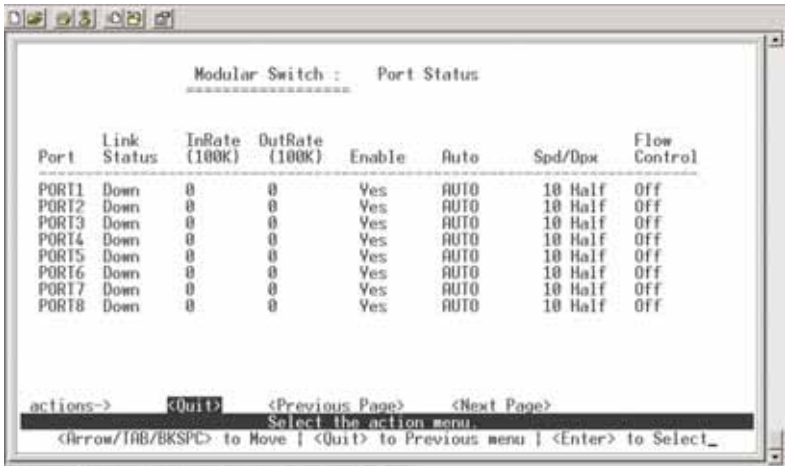
Enabled: Shows whether the port is enabled or disabled. Depending on the user's setting a "Yes" or "No" status will be displayed respectively. If the port is not linked its status be treated as "No".

Auto: Displays the port NWay link mode: Auto, NWay_Force, Force.

Spd/Dpx: Displays the port speed and duplex.

FlowCtrl: In auto / NWay force mode, the display for the flow control status is enabled or disabled on auto-negotiation. In force mode, the display for flow control status is

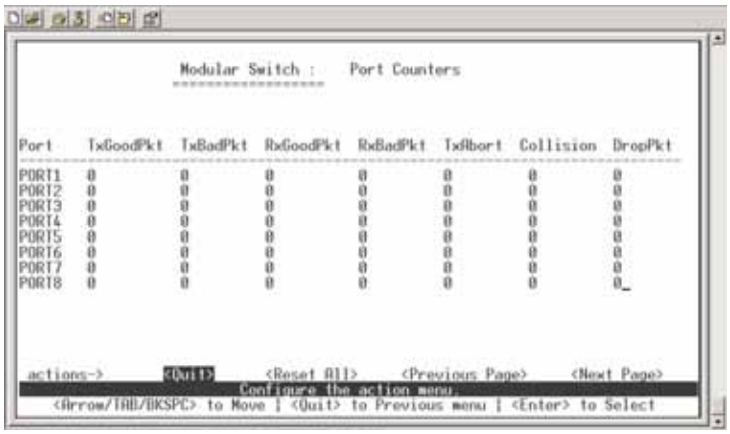
enabled or disabled depending on the user's setting.



<Quit>: Exit the port status page, and return to the previous menu.
<Previous Page>: Display previous page.
<Next page>: Display next page.

4-4-2. Port Counters

The following information provides a view of the current status of the unit.
<Quit>: Exit the port status page and return to previous menu.
<Reset All>: Set all counts to 0.
<Previous Page>: Display previous page.
<Next page>: Display next page.



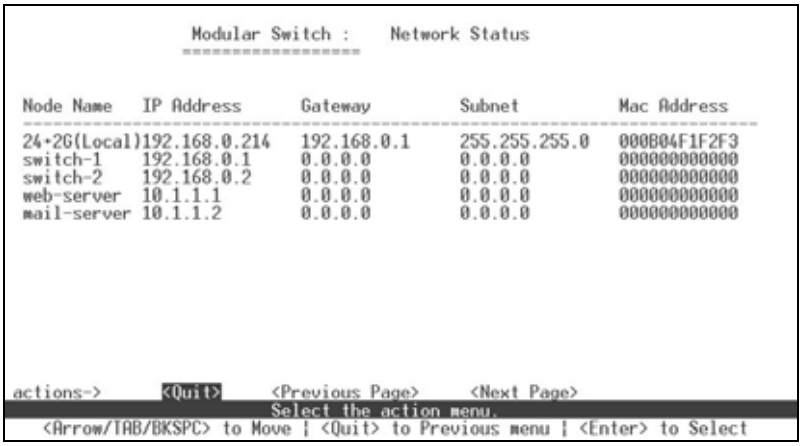
4-4-3. System Information

MAC Address: Media Access Control - The unique hardware address assigned by manufacturer.

Firmware Version: Display the Switch's firmware version.

4-4-4. Network Information

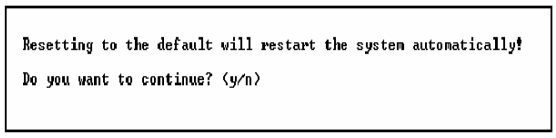
Display network devices IP address, Gateway address, MAC Address, and Subnet mask from the Network Status page.



4-5. Reboot Switch

4-5-1. Default

Reset Switch to default configurations.



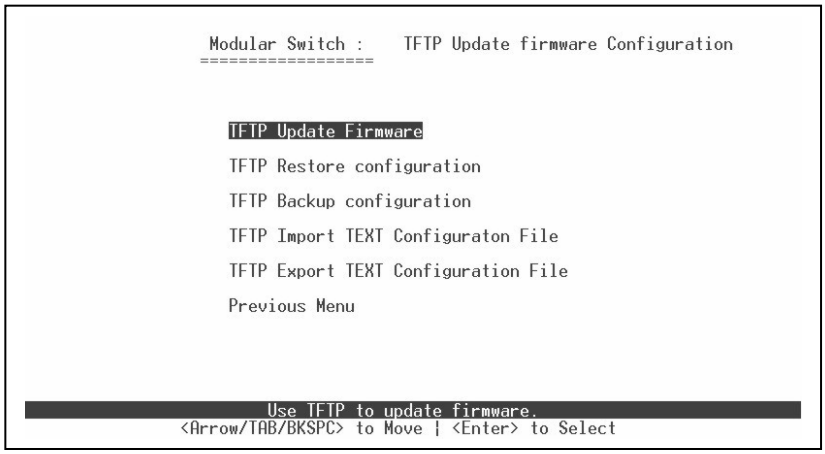
You will be prompted with the above message. Press “Y” to load default setting after reboot. After loading default settings, the Switch will reboot automatically.

4-5-2. Restart

Reboots the Switch with a software reset.

4-6. TFTP Update Firmware

Use this page to update firmware, restore EEPROM values, or upload (save) current EEPROM values.


Modular Switch : TFTP Update firmware Configuration
TFTP Update Firmware
TFTP Restore configuration
TFTP Backup configuration
TFTP Import TEXT Configuraton File
TFTP Export TEXT Configuration File
Previous Menu
Use TFTP to update firmware.
<Arrow/TAB/BKSPC> to Move | <Enter> to Select

4-6-1. TFTP Update Firmware

Use the TFTP Update firmware Configuration page to update firmware via TFTP

1. Start the TFTP server, and copy firmware update version image file to TFTP server.
2. Select **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **<Save>**, the Switch will start to download the image file.
7. When the update is successful, the image file will be downloaded.
8. Restart the Switch to launch the version of firmware.

4-6-2. Restore Configuration File

Use the TFTP Update Firmware page to restore EEPROM values from a saved image file located on a TFTP server.

1. Start the TFTP server.
2. Select **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.

4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **<Save>.** The Switch will start to download the image file.
8. When the restore function is successful, the image is downloaded.
9. Restart the Switch to resume normal operations.

4-6-3. Backup Configuration File

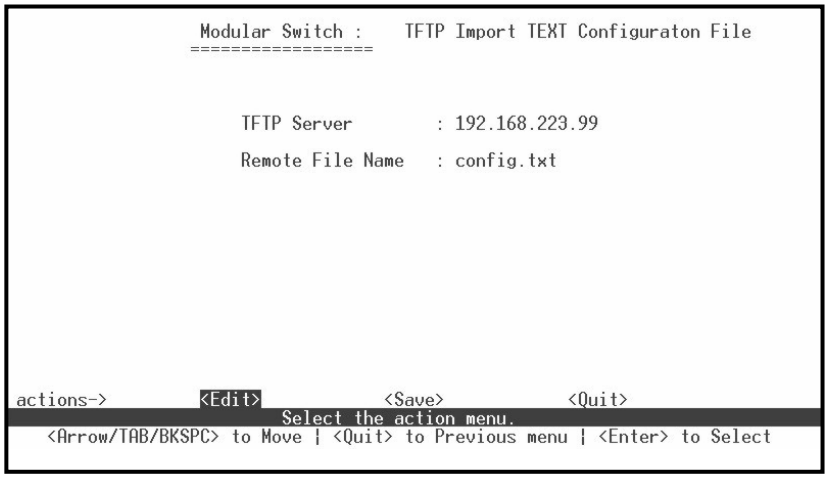
Use the Backup Configuration File page to save the current EEPROM value to image file. Then when necessary, go to the update configure page to retrieve the EEPROM value.

1. Start the TFTP server.
2. Select **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **<Save>.** The Switch will start to save the image file.
6. When backup function successfully, the image file is saved to the designated TFTP server.
7. Follow the instructions given in the Restore Configure File page to restore lost settings

4-6-4. TFTP Import Text Configuration File

Use the TFTP Import TEXT Configuration File page to restore EEPROM value from a saved text file in a TFTP server.

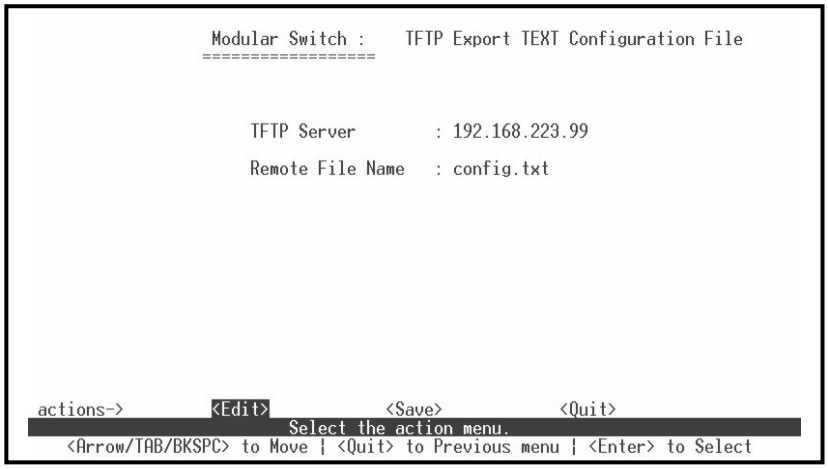
1. Start the TFTP server.
2. Select **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the text file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **<Save>.** The Switch will start to download the text file.
7. When the restore function is successful, the image is downloaded. If there is any error, you would see a Report.txt file in the TFTP server. The configurations might be partial installed if the importing procedure has any error.
8. It is suggested that you restart the Switch to resume normal operations.



4-6-5. TFTP Export Text Configuration File

Use the TFTP Export Text Configuration File page to save the current EEPROM value to a text file.

1. Start the TFTP server.
2. Select **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** to go to the action line.
6. Select **<Save>.** The Switch will start to save the image file.
7. When Export function successfully, the image file is saved to the designated TFTP server.
8. Follow the instructions given in the TFTP Import Configuration File page to restore settings


Modular Switch : TFTP Export TEXT Configuration File
TFTP Server : 192.168.223.99
Remote File Name : config.txt
actions-> <Edit> <Save> <Quit>
Select the action menu.
<Arrow/TAB/BKSPC> to Move | <Quit> to Previous menu | <Enter> to Select

5 Menu-Driven Interface via Telnet

This section provides some basic instructions to using Menu-Driven Interface to configure the Switch. Follow the instructions below:

1. Open a Command Prompt window and type

   telnet xxx.xxx.xxx.xxx where xxx represents the IP address.

   As an example, we'll continue to use the IP address configured in part A of this manual: 192.168.0.197

2. Then "**Press <ENTER> key to start**"

3. The default Login name is "admin" with no preset password.
   The system provides a menu-driven user interfaces via console or telnet. After you log into the system, you will see a window similar to that as the console interface like in the section one. To use the management facilities of the Switch via telnet, please see section four.

6 Troubleshooting

The network administrator can observe and monitor most areas of the Switch status using the LED indicators on the front panel to quickly identify problems. This section contains a few of the more common problems that may arise and possible solutions.

Symptom: Power indicator does not light up after power on.
Cause: Defective power outlet, power cord or internal power supply.
Solution: Verify if the power outlet is functioning normally by plugging in another properly operating device. Connect the power cord to another device to test. If these two tests fail to resolve the problem, replace the power supply unit.

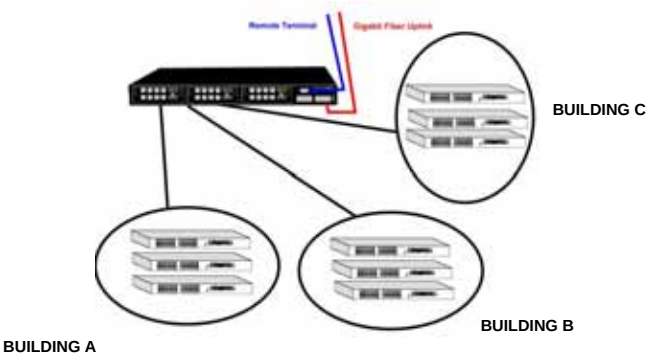
Symptom: Link indicator does not light up after making a connection.
Cause: Network cable or fiber switch port is defective.
Solution: Ensuring that the attached device and switch are powered on. Verify the fiber cable has been properly connected to both devices. Review that the cabling distance does not exceed specified limits. Inspect cable for defects and replace if necessary.

Symptom: Unit powers off during operation after a period of time.
Cause: Loose power connections, power surges/loss or inadequate ventilation.
Solution: Ensure that all power connections are secured and the unit fans have proper ventilation. If unable to correct the problem by above measures, it may be necessary to replace internal power supply unit.

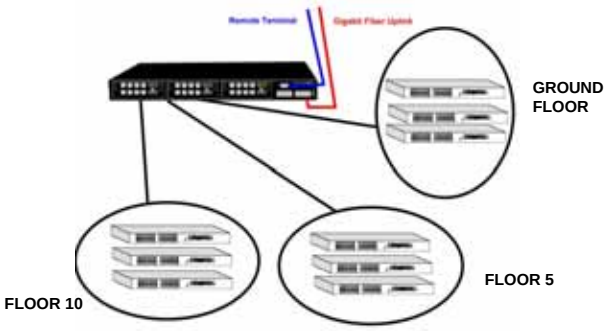
Appendix A

Application Examples

Building to Building (Small Campus)
In the figure below, the Switch is functioning as a backbone for a small campus network configuration. It is providing a max. of 200 Mbps full duplex link to a remote stack of 10/100 switches.

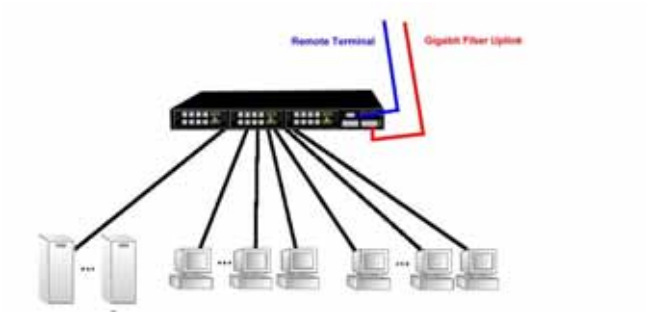


Enterprise Server Aggregation
Using the same basic topology as above, only providing access to workgroups of 10/100 switches located on separate floors within a single building.



LAN Switch

In the figure below, the Switch is functioning as a high-speed bridge between segments creating increased capacity for each user (node) on the local area network. It is providing a 200 Mbps full duplex link to a variety of Ethernet / Fast Ethernet network devices within a LAN.



UP TO 24 NETWORK NODES CONNECTED
-10/100Mbps over copper segments
-100Mbps over fiber segments

Appendix B

802.1q Tag-VLAN Application Example

An IEEE 802.1q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN. Figure 1 demonstrates a VLAN example with two switches and four VLAN groups. Below are details and configuration steps.

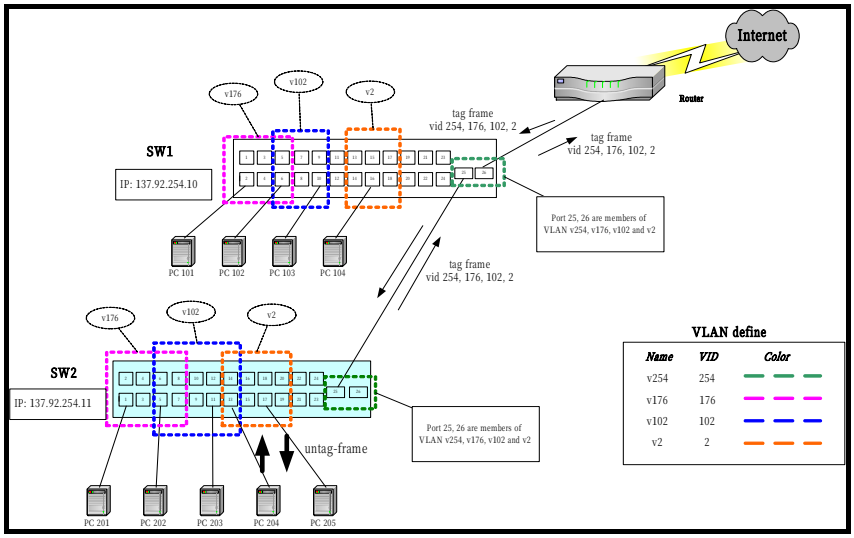


Figure 1. 802.1q Tag-VLAN example

Network Topology

In Fig 1, we will have a fiber (1000SX) carrying tagged VLANs with trivial VIDs (254,176,102,2) only. This will be connected to the uplink port (26) on a switch SW1. The internal management interface of this SW1 will have an IP address on VLAN VID 254 (e.g. 137.92.254.10). A 1000SX port (25) on this SW1 will then be connected to the uplink port (26) on SW2 and it will carry tagged packets VIDS (254.176.102.2). Again the management port of the SW2 will be on VLANs VID 254 (e.g. 137.92.254.11). We will have a few ports on the Switch to egress untagged packets on VLANs 254.76.102.2. And we can telnet/SNMP the management interfaces of both the SW1 and the SW2. A laptop on either VLANs 254.176.102.3 can see the rest of the network(s).

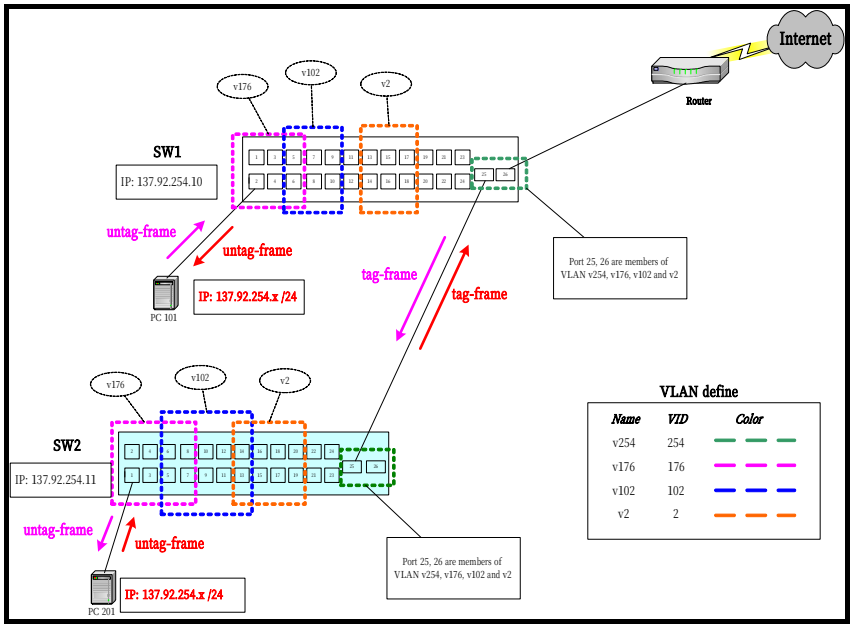
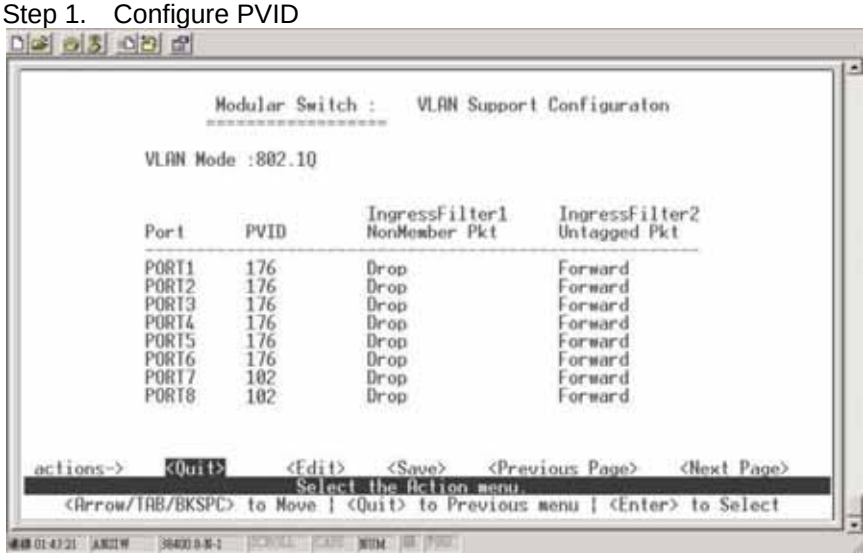


Figure 2. Communications between PC101 & PC201 with tagged-VLAN.

802.1q Tag-VLAN Switch Configuration – Using Menu Driven

Switch 1 Configuration Steps

Step 1. Configure PVID



[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [VLAN Configure]
Select VLAN mode (802.1q)

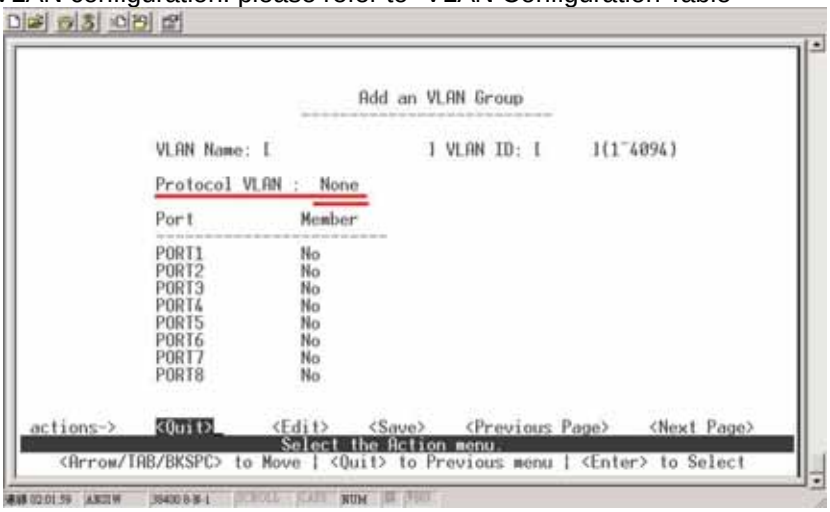
PVID Configuration: please refer to “PVID Configuration Table”

PVID Configuration Table	
PVID	**Port #**
176	1~6
102	7~10
2	13~18
254	25, 26
1 (default)	11,12,19~24

Step 2. Create VLAN Group: v176, 102, v2, v254

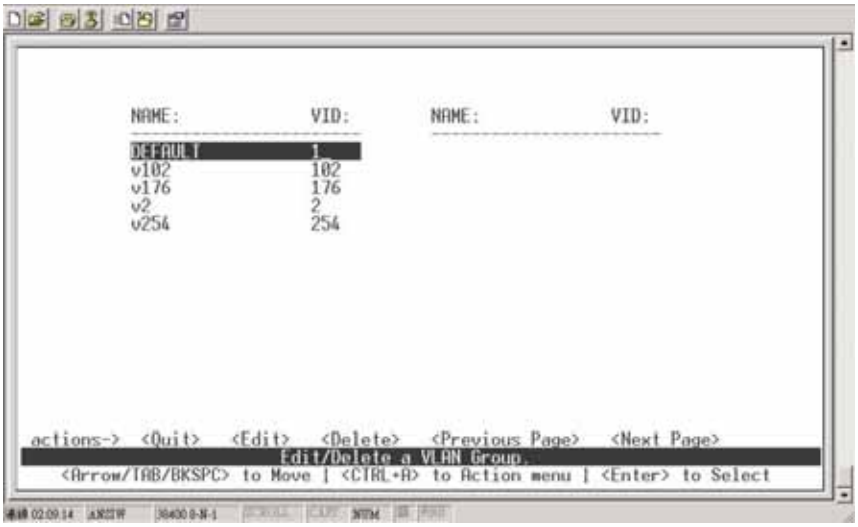
[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [Create a VLAN Group]

VLAN configuration: please refer to “VLAN Configuration Table”



VLAN Configuration Table				
VLAN Config.		**Port Member (port #)**		
Name	***VID***	***untagged***	***tagged***	***no***
Default	1	11, 12, 21~24	25, 26	else
v176	176	1~6	25, 26	else
v102	102	5~10	25, 26	else
v2	2	13~18	25, 26	else
v254	254	✕	25, 26	else

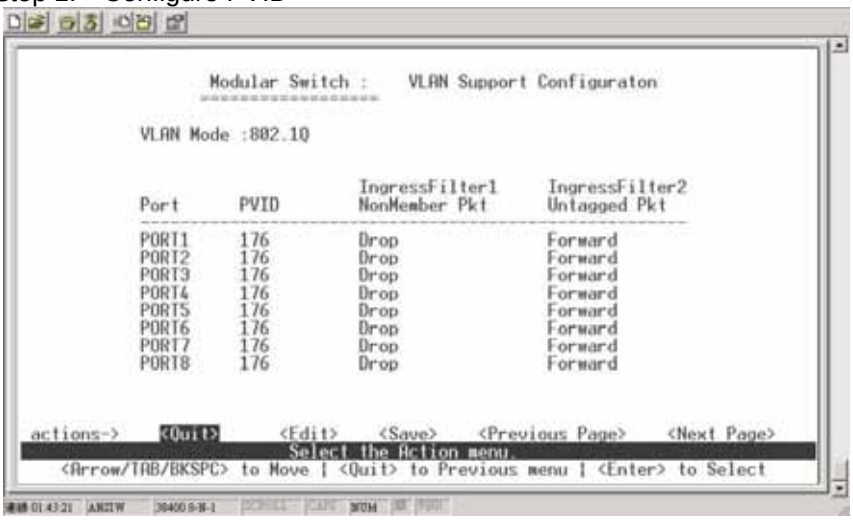
Step 3. Edit “Default” VLANs



[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [Edit/Delete a VLAN Group]
VLAN configuration: please refer to “VLAN Configuration Table” above.

Switch 2 Configuration Steps

Step 1. Configure PVID



[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [VLAN Configure]
Select VLAN mode (802.1q)

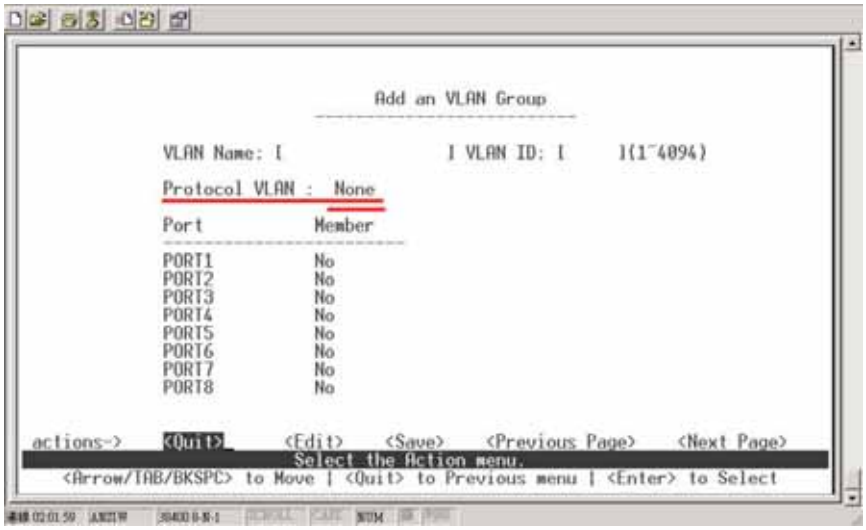
PVID configuration: please refer to “PVID Configuration Table”

PVID Configuration Table	
PVID	**Port #**
176	1~8
102	9~14
2	15~20
254	25, 26
1 (default)	21~24

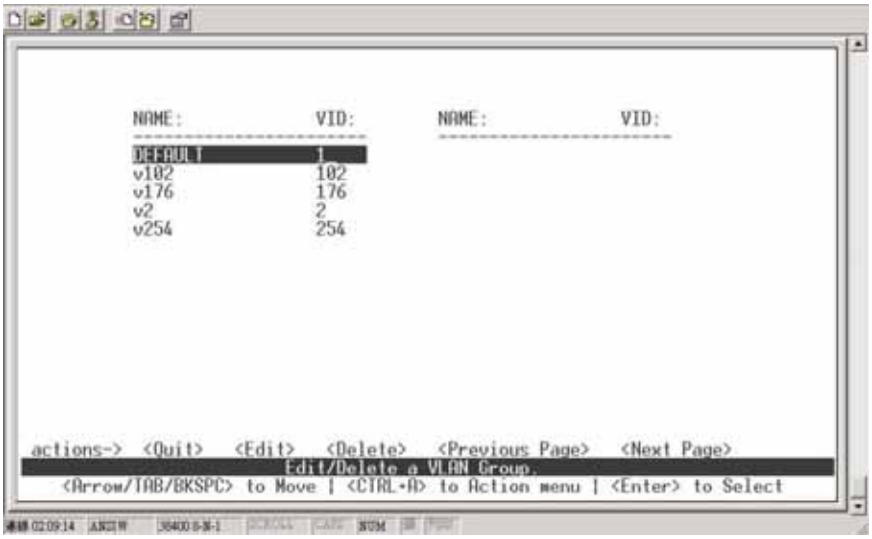
Step 2 . Create VLAN Group : v176, 102, v2, v254
[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [Create a VLAN Group]

VLAN configuration: please refer to “VLAN Configuration Table”

VLAN Configuration Table				
VLAN Config.		**Port Member (port #)**		
Name	***VID***	***untagged***	***tagged***	***no***
Default	1	21~24	25, 26	else
v176	176	1~8	25, 26	else
v102	102	5~14	25, 26	else
v2	2	13~20	25, 26	else
v254	254	×	25, 26	else



Step 3. Edit “Default” VLANs



[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨[Edit/Delete a VLAN Group]

VLAN configuration: please refer to “VLAN Configuration Table” above.

Connecting VLAN Groups

The Switch supports communication within a common VLAN. However, if you have devices in separate VLANs that need to communicate, and it is not practical to include these devices in a common VLAN, and then the VLANs can be connected via the Layer 3 routing provided by another Layer 3 switch. In Fig 3, we use the router with two network interfaces (192.168.0.1 /24, 192.168.1.1 /24) to provide the Layer 3 routing.

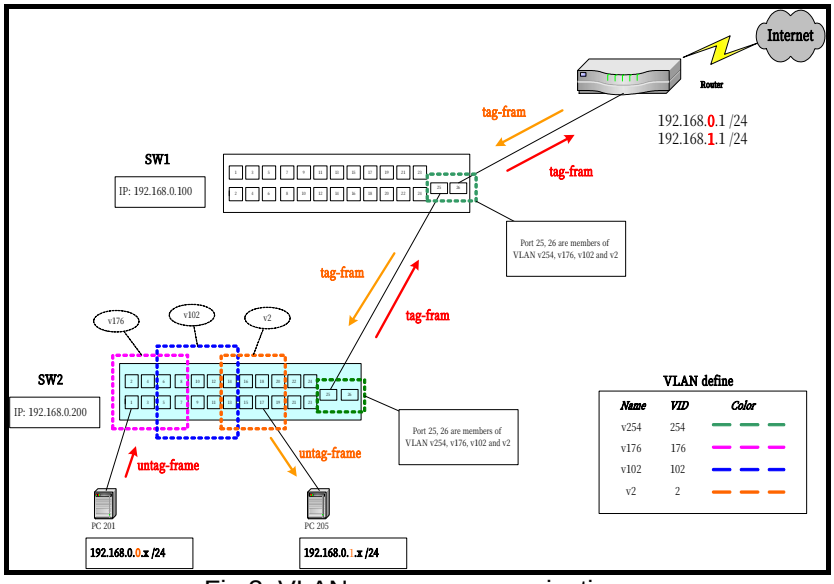


Fig 3. VLAN groups communication.

Appendix C

Protocol VLAN Application Example

In order for an end station to send packets to different VLANs, itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol. The Protocol-based VLAN feature of the Switch can be applied for accommodating devices that you want to participate in the VLAN by means of built-in knowledge of layer 2 packet formats used by selected popular protocols, such as IP and Novell IPX. The following example will demonstrate you how to configure the Switch for protocol—based VLAN application.

Figure 1 shows two switches with workstations and servers which are going to work by using protocol VLAN.

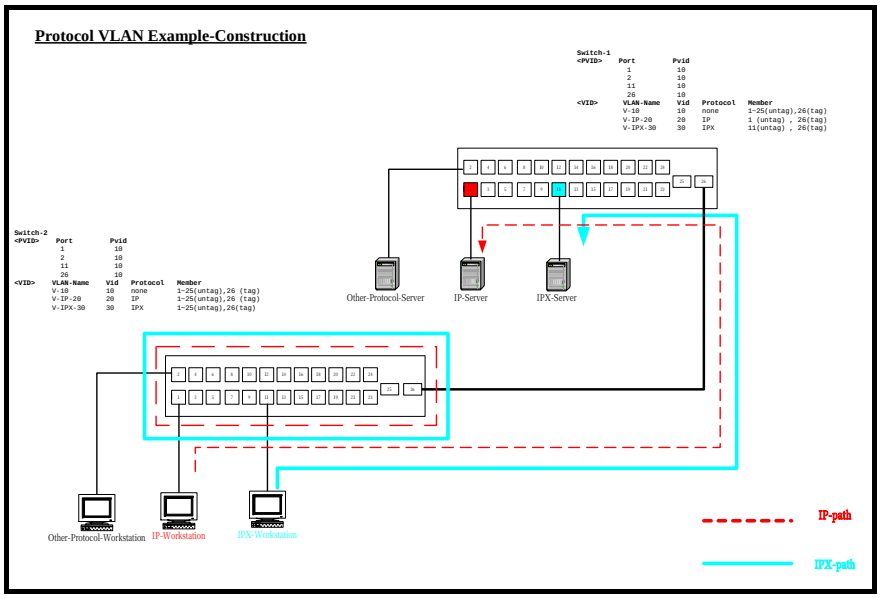


Figure 1. Protocol VLAN Example

Figure 2 shows you the internal settings and data flows in the switches. In this application, the IP packets from workstations will go to the IP server only and the IPX packets will go to the IPX server only.

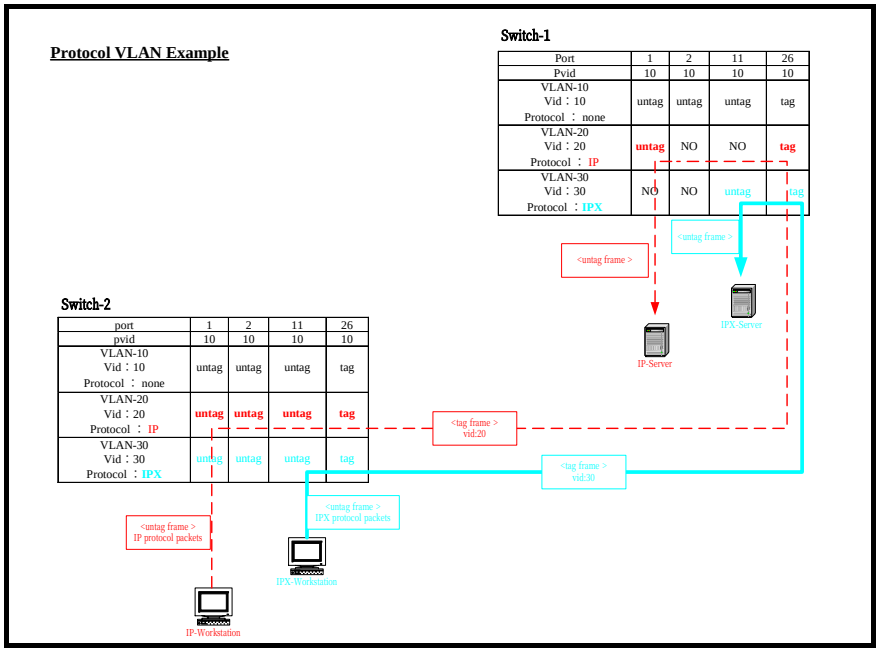
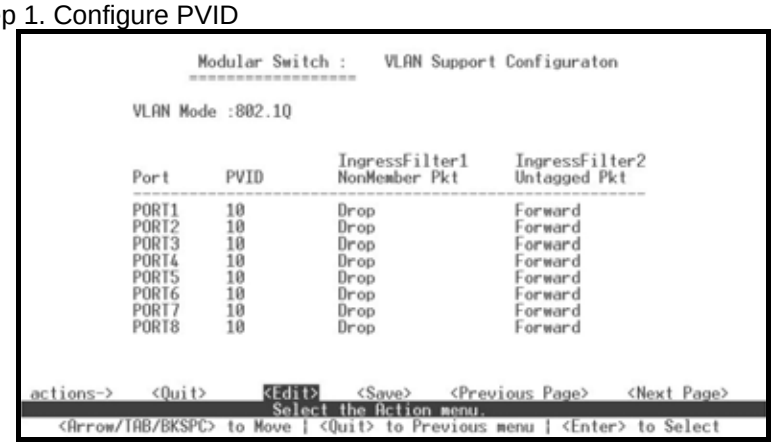


Figure 2. Protocol VLAN Example

Switch 1 Configuration Steps

Step 1. Configure PVID

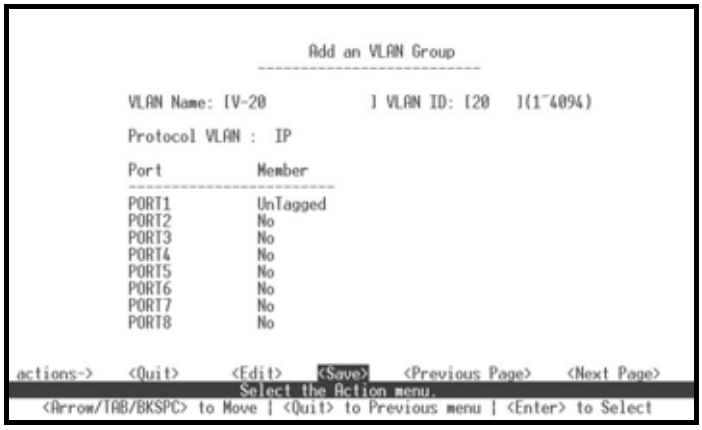


[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [VLAN Configure]
Select VLAN mode (802.1q)

PVID configuration: please refer to “PVID Configuration Table”

PVID Configuration Table	
PVID	**Port #**
10	1~26

Step 2 . Create VLAN Group : V-10, V-IP-20, V-IPX-30



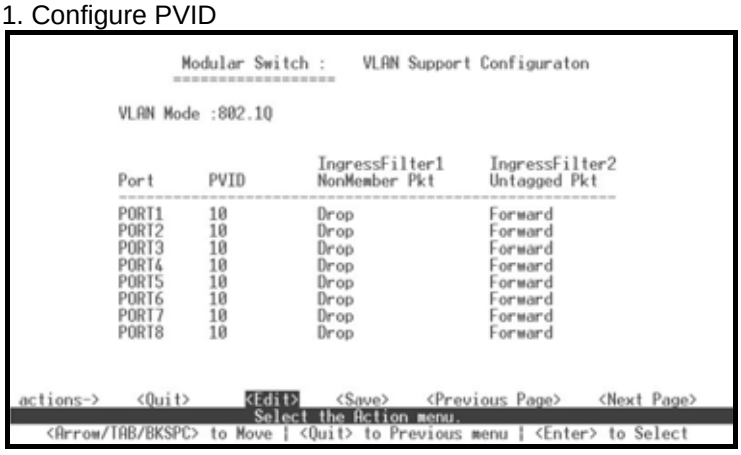
[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [Create a VLAN Group]

VLAN configuration: please refer to “VLAN Configuration Table”

VLAN Configuration Table					
VLAN Config.			**Port Member (port #)**		
Name	***VID***	***Protocol***	***untagged***	***tagged***	***no***
Default	1	None	X	X	1~26
V-10	10	None	1~25	26	X
V-IP-20	20	Ip	1	26	else
V-IPX-30	30	Ipx	11	26	else

Switch 2 Configuration Steps

Step 1. Configure PVID

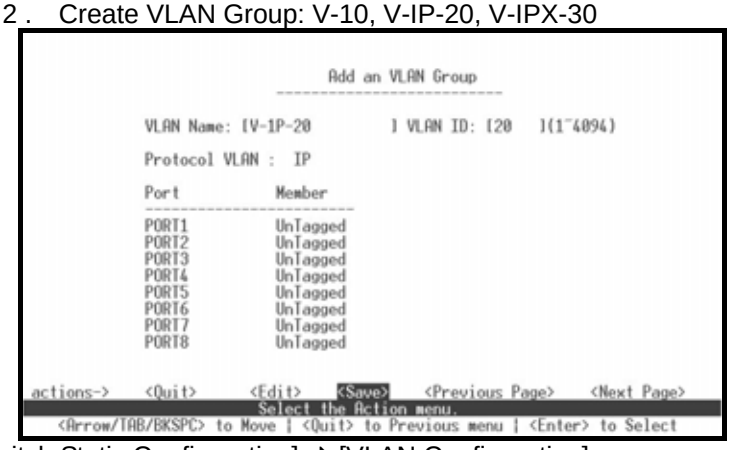


[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [VLAN Configure]
Select VLAN mode (802.1q)

PVID configuration: please refer to “PVID Configuration Table”

PVID Configuration Table	
PVID	**Port #**
10	1~26

Step 2 . Create VLAN Group: V-10, V-IP-20, V-IPX-30



[Switch Static Configuration] ⇨ [VLAN Configuration]
⇨ [Create a VLAN Group]

VLAN configuration: please refer to “VLAN Configuration Table”

VLAN Configuration Table					
VLAN Config.			**Port Member (port #)**		
Name	***VID***	***Protocol***	***untagged***	***tagged***	***no***
Default	1	None	X	X	1~26
V-10	10	None	1~25	26	X
V-IP-20	20	Ip	1~25	26	X
V-IPX-30	30	Ipx	1~25	26	X

Appendix D

System Configuration File Example

```
[BEGIN]

[PORT_CONFIG]
//PORT CONFIGURATION
//Port ID=1,2,...26
//Ingress Rate Control(InRate): 0,1,2...1000
//Egress Rate Control(OutRate): 0,1,2...1000
//State Enable(STATE): YES/NO
//Auto Negotiation(AUTO):    AUTO/NWAY-FORCE/FORCE (GigaPort: AUTO/FORCE)
//Speed&Duplex(SPD&DPX): 10HALF/10FULL/100HALF/100FULL (GigaPort:
1000HALF/1000FULL)
//Flow-Control of Full Duplex(FCFD): ON/OFF
//Flow-Control of Half Duplex(FCHD): ON/OFF
//port ID,"=", InRate, OutRate, STATE,AUTO, SPD&DPX, FCFD, FCHD
1 = 0,0,YES,AUTO,100FULL,ON,ON
2 = 10,20,YES,NWAY-FORCE,10HALF,OFF,ON
3 = 0,0,NO,FORCE,10FULL,ON,OFF
4 = 0,0,YES,AUTO,100HALF,ON,ON
5 = 0,0,YES,AUTO,100FULL,ON,ON
6 = 0,0,YES,AUTO,100FULL,ON,ON
7 = 0,0,YES,AUTO,100FULL,ON,ON
8 = 0,0,YES,AUTO,100FULL,ON,ON
9 = 0,0,YES,AUTO,100FULL,ON,ON
10 = 0,0,YES,AUTO,100FULL,ON,ON
11 = 0,0,YES,AUTO,100FULL,ON,ON
12 = 0,0,YES,AUTO,100FULL,ON,ON
13 = 0,0,YES,AUTO,100FULL,ON,ON
14 = 0,0,YES,AUTO,100FULL,ON,ON
15 = 0,0,YES,AUTO,100FULL,ON,ON
16 = 0,0,YES,AUTO,100FULL,ON,ON
17 = 0,0,YES,AUTO,100FULL,ON,ON
18 = 0,0,YES,AUTO,100FULL,ON,ON
19 = 0,0,YES,AUTO,100FULL,ON,ON
20 = 0,0,YES,AUTO,100FULL,ON,ON
21 = 0,0,YES,AUTO,100FULL,ON,ON
22 = 0,0,YES,AUTO,100FULL,ON,ON
23 = 0,0,YES,AUTO,100FULL,ON,ON
24 = 0,0,YES,AUTO,100FULL,ON,ON

[VLAN_MODE]
//VLAN_MODE = 802.1Q/PORTBASE/DISABLE
VLAN_MODE = 802.1Q

[VLAN_PORT]
```

```
//PVID: 1~4095(MUST IN SAME RANGE, e.g. 1~255, 256~511, ...)
//INGRESSFILTER1 NONMEMBER PKT: DROP/FORWARD
//INGRESSFILTER2 UNTAGGED PKT: DROP/FORWARD
//port ID, "=", PVID, IngressFilter 1, Ingress filter 2
1 = 1,DROP,FORWARD
2 = 2,DROP,DROP
3 = 3,FORWARD,DROP
4 = 4,FORWARD,FORWARD
5 = 1,DROP,FORWARD
6 = 1,DROP,FORWARD
7 = 1,DROP,FORWARD
8 = 1,DROP,FORWARD
9 = 1,DROP,FORWARD
10 = 1,DROP,FORWARD
11 = 1,DROP,FORWARD
12 = 1,DROP,FORWARD
13 = 1,DROP,FORWARD
14 = 1,DROP,FORWARD
15 = 1,DROP,FORWARD
16 = 2,DROP,FORWARD
17 = 1,DROP,FORWARD
18 = 1,DROP,FORWARD
19 = 1,DROP,FORWARD
20 = 1,DROP,FORWARD
21 = 1,DROP,FORWARD
22 = 1,DROP,FORWARD
23 = 1,DROP,FORWARD
24 = 1,DROP,FORWARD

[VLAN_802.1Q]
//VLAN_NAME: A string less than 8 characters
//VLAN_ID: 1,2,...4095
//TAG_MEMBER:1,2,...26
//UNTAG_MEMBER:1,2,...26
//PROTOCAL VLAN (PROTOCAL TYPE):NONE/IP/ARP/APPLETALK-NETBIOS/
//              APPLETALK-AARP-IOS-NETWORK-LAYER-PDU/NOVELL-IPX/
//
BANYAN-VINES-NOVELL-IPX(RAW-ETHERNET)/BANYAN-VINES-STP-BPDU/
//              BANYAN-VINES-NULL-SAP/DECNET-MOP/DECNET-MOP/DECNET-DPR/
//              DECNET-LAT/DECNET-LAVC/IBM-SNA/X.75-INTERNET/X.25-LAYER3
VLAN_NAME = DEFAULT
VLAN_ID = 1
TAG_MEMBER =
UNTAG_MEMBER = 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
PROTOCAL_VLAN = NONE

[VLAN_802.1Q]
VLAN_NAME = TEST02
VLAN_ID = 2
TAG_MEMBER = 1,3
UNTAG_MEMBER = 2,5
PROTOCAL_VLAN = NONE
```

```
[VLAN_802.1Q]
VLAN_NAME = TEST03
VLAN_ID = 3
TAG_MEMBER = 7,8
UNTAG_MEMBER = 1,2,3
PROTOCAL_VLAN = APPLETALK-NETBIOS

[VLAN_802.1Q]
VLAN_NAME = TEST04
VLAN_ID = 4
TAG_MEMBER = 21,22,23
UNTAG_MEMBER = 10,11
PROTOCAL_VLAN = IBM-SNA

[END]
```

Contact Us

VOLKTEK CORPORATION
4F, No. 192 Lian-Cheng Road
Chung-Ho, Taipei 235, Taiwan ROC
TEL: +86 (2) 8242-1000
FAX: +886 (2) 8242-3333
Tech Support: +886 800-286-286
ISO 9001 Certified